2018

Contributions to Attribute-Based Encryption and Its Variants

Yinhao Jiang
University of Wollongong

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Contributions to Attribute-Based Encryption and Its Variants

Yinhao Jiang

Supervisor:
Prof. Willy Susilo
Co-supervisors:
Prof. Yi Mu, Dr. Fuchun Guo

This thesis is presented as required for the conferral of the degree:

Doctor of Philosophy

The University of Wollongong
School of Computing and Information Technology

June 6, 2018

Declaration

I, Yinhao Jiang, declare that this thesis submitted in fulfilment of the requirements for the conferral of the degree Doctor of Philosophy, from the University of Wollongong, is wholly my own work unless otherwise referenced or acknowledged. This document has not been submitted for qualifications at any other academic institution.

Yinhao Jiang
June 6, 2018

Abstract

Attribute-based encryption (ABE) as a promising cryptographic primitive in public-key cryptography is faced with many challenges from inherent incompatible construction difficulties and demands of real-world applications.

This thesis starts from the study of efficiency and expressiveness of attribute-based encryption. The feature of flexibility of attribute-based encryption causes additional computational overheads in encryption and decryption and increases the length of ciphertexts and private keys. The dilemma between efficiency and expressiveness of attribute-based encryption encourages novel techniques in ABE scheme construction. A new ciphertext-policy attribute-based encryption (CP-ABE) scheme supporting access policies of an AND-gate and a threshold with short ciphertexts is proposed. Such a scheme offers succinct ciphertexts with further expressiveness and allows encryptors to assign attributes into types of mandatory and optional when designing an access policy.

An insightful observation of key construction in CP-ABE systems leads to an interesting topic of key-delegation abuse. This issue shows a property of CP-ABE schemes that without further restriction any valid user private key can be used to delegate new keys with less access privilege. Considering possible severe consequence, a new CP-ABE scheme with key-delegation abuse resistance is proposed. Such a scheme prohibits illegally generating new keys by any kind of splitting or combining user private keys.

The thesis then investigates a new challenge of access policy update in ABE systems. The access policies in private keys or ciphertexts in ABE systems cannot be changed; however, the ability of modifying existing policies is highly desired for real-world applications. Schemes with efficient attribute addition and revocation mechanism are proposed. Such schemes allow encryptors to add (or revoke) attributes to (or from) access policies of existing ciphertexts via a proxy server and remain the ciphertexts sent to users with constant size.

The thesis further conducts research into real-world scenarios. The scenario of Fog Computing is first considered and a traceable CP-ABE scheme with key-delegation abuse resistance is proposed to solve private key delegation and key duplication problem. The second considered scenario is the problem of preserving certain attributes when applying the proposed access policy update mechanism. We propose two innovative CP-ABE schemes and their variants for scenarios in Fog Computing and access policy update with attribute preservation.

Acknowledgements

This thesis would have been impossible without the support and advice of my supervisors: Willy Susilo, Yi Mu, and Fuchun Guo. I would like to express my deep gratitude to them for their excellent guidance, insightful discussions and constant encouragement through all the stages.

I would like to express my thanks to Guomin Yang, Nan Li, Hui Cui, Rongmao Chen, Jongkil Kim, Clementine Gritti, Shiwei Zhang, Tran Viet Xuan Phuong, Jianchang Lai and Arnaud Sipasseuth for their critical comments and valuable input to my study. Their intuitive feedback on my research work have supported me in my three years' PhD learning. I would like to express my thanks to all the members in the Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, for their company in my PhD study.

I would like to express my thanks to all my friends in Australia, a non-exhaustive list of whom includes: Dany Aguera Zurdo, Wence Peraza, Nina Skyrud, Idin Borhai, Kamilla Chmielewski, Mahan Karimani, Xiaochen He, Mengnan Li, Guanqiao Huang, Ziwei Ke, Philia Pu for their help and company when living in Australia.

I would like to express my appreciation to my family, my father Zheng Jiang and my mother Minghong Tang, for their enormous help and support. I would also like to express my thanks to my uncle Sheng Tang. I wish him the might and courage to fight against cancer.

Finally, I would like to appreciate Xin Gao.

Publications

This thesis is related to the following publications/manuscripts.

1. **Yinhao Jiang**, Willy Susilo, Yi Mu, and Fuchun Guo. "Ciphertext-Policy Attribute-Based Encryption Supporting Access Policy Update and Its Extension with Preserved Attributes. International Journal of Information Security, August 7, 2017. doi:10.1007/s10207-017-0388-7.

2. **Yinhao Jiang**, Willy Susilo, Yi Mu, and Fuchun Guo. "Flexible Ciphertext-Policy Attribute-Based Encryption Supporting AND-Gate and Threshold with Short Ciphertexts. International Journal of Information Security, May 17, 2017. doi:10.1007/s10207-017-0376-y.

3. **Yinhao Jiang**, Willy Susilo, Yi Mu, and Fuchun Guo. "Ciphertext-Policy Attribute-Based Encryption against Key-Delegation Abuse in Fog Computing. Future Generation Computer Systems, January 2017. doi:10.1016/j.future.2017.01.026.

4. **Yinhao Jiang**, Willy Susilo, Yi Mu, and Fuchun Guo. "Ciphertext-Policy Attribute-Based Encryption Supporting Access Policy Update." In International Conference on Provable Security, pp. 39-60. Springer International Publishing, 2016.

5. **Yinhao Jiang**, Willy Susilo, Yi Mu, and Fuchun Guo. "Ciphertext-Policy Attribute-Based Encryption with Key-Delegation Abuse Resistance." In Australasian Conference on Information Security and Privacy, pp. 477-494. Springer International Publishing, 2016.

List of Notations

The following abbreviations are used throughout this thesis.

A	An attribute
A_i	The i-th attribute in an attribute universe
$\mathbb{A}$	An access structure
$\mathsf{Adv}_{\mathcal{B}}^{\mathcal{Y}}$	The advantage probability of the event that $\mathcal{B}$ wins in $\mathcal{Y}$
CT	A ciphertext
$\deg B$	The degree of B
$\mathbb{G}$	A group
λ	A security parameter
1^λ	A string of length λ
M	A message
$\mathcal{P}$	An attribute universe
$\Pr[X]$	The probability that event X happens
sk	A private key
$W \models \mathbb{A}$	A set of attributes W satisfies the access structure $\mathbb{A}$
$W \not\models \mathbb{A}$	A set of attributes W does not satisfy the access structure $\mathbb{A}$
$x \notin X$	x is not in set X
$\mathbb{Z}$	The set of integers
$\mathbb{Z}_p$	The set of integers modulo p: $\{0, 1, 2, \ldots, p-1\}$

List of Abbreviations

The following abbreviations will be used in this thesis. Some special abbreviations will be defined when they are first used.

ABE	Attribute-Based Encryption
A^2BE	Accountable Attribute-Based Encryption
A^3BE	Accountable and Anonymous Attribute-Based Encryption
APU	Access Policy Update
AFKP	Abuse Free Key-Policy
CP	Ciphertext-Policy
CCA	Chosen Ciphertext Attacks
CPA	Chosen Plaintext Attacks
D-linear	Decision Linear
DDH	Decisional Diffie-Hellman
DBDH	Decisional Bilinear Diffie-Hellman
GDHE	General Diffie-Hellman Exponent
IBE	Identity-Based Encryption
IND	Indistinguishability
KP	Key-Policy
LSSS	Linear Secret Sharing Scheme
PRE	Proxy Re-Encryption
PKG	Private Key Generator
3P-SDP	Subgroup Decision Problem for 3 Primes
SAA	Stand-Alone Authentication
aMSE	Augmented Multi-Sequence Exponent
sCPA	Selective Chosen Plaintext Attacks

[This page is intentionally left blank]

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Attribute-based encryption (ABE) challenges cryptographers to construct efficient, expressive and versatile one-to-many encryption schemes. The notion was introduced by Sahai and Waters [SW05] shortly after the first concrete identity-based encryption (IBE) [BF01a] scheme was proposed. An IBE system is a special public key encryption system where messages are encrypted with public keys and recovered with secret keys. Identities of users, which are usually strings and known by each other, took the role of public keys in IBE so that messages can be encrypted without key establishment – i.e., given a ciphertext CT_{ID} encrypted with identity ID and a private key $sk_{ID'}$ generated for identity ID', one can recovers the message from CT_{ID} using $sk_{ID'}$ if and only if ID is identical to ID'. This condition of being equivalent of identities in decryption restricts IBE in the type of inflexible one-to-one encryption, which led to a natural question proposed by Sahai and Waters [SW05]: Is it possible to redefine the identities of users so that the decryption condition can then be extended to richer types of functions or more expressive access controls? They answered the question positively by replacing identities of users by descriptive attributes. The encryption was then no longer based on strings of inseparable identities but relatively independent attributes, which made it possible to successfully decrypt one ciphertext using one of many different private keys that satisfy the decryption condition.

ABE schemes features a one-to-many encryption mode with integrated access control that complies with the developing Internet: first, it resolves the dilemma between the security of sensitive data and the capability to manage its access control in many scenarios; second, its flexibility as one step further beyond traditional "all or nothing" encryption can efficiently adapt the dynamic environment. In addition, ABE can be further extended for numerical computation access control or utilities of further complex functions, as functional encryption, to meet future challenges.

This research focuses on constructing efficient ABE schemes with improved expressiveness and different versatilities. Specifically, our research addresses "roadblocks" to real world applications faced by different variants of ABE, such as computational overheads, inherent defects in key management and adjustable access control management. This research also focuses on the applications and deployments of different ABE schemes in assorted challenging scenarios.

1.1 Motivation and Objective

In this section, we present our motivations and corresponding objectives.

1.1.1 Efficiency and Expressiveness

With the development of communication networks, there is a trend for users to transmit sensitive data on the Internet. To distribute a message to a specific set of users, a trivial method is to encrypt it under each user's public key or identity in traditional cryptosystem. As expected, ciphertext size and computational cost of encryption or decryption algorithms are linear with the number of receivers. Therefore, it is less attractive or even intolerable when the number of receivers is large.

On the other hand, establishing a specific access control policy can also be deployed for sensitive data transmission since most of the recipients can be categorised according to many common attributes, such as gender, age range, and position. This type of expressive access control is usually enforced by employing a trusted server to store data locally, of which the security becomes increasingly difficult to be guaranteed due to replications caused by the distributed fashion of data storage. Hence, sensitive data is required to be stored in an encrypted form and the access control becomes pointless.

Attribute-based encryption tackles the problem by enforcing encrypted data to be decrypted with a secure access control mechanism. ABE expands the traditional understanding of public-key cryptography by allowing the public-key to be not atomic but associated with sets of attributes. In an ABE system, users' keys and ciphertexts are labelled with sets of descriptive attributes and decryption conditions. A ciphertext can be decrypted only if the attributes of the ciphertext and/or the user's key satisfies certain conditions where user keys are always issued by a trusted party. However, the way ABE enforces access control brings inconvenience to the construction of encryption schemes. The user keys and ciphertexts in ABE system contain more components according to labelled attributes, which itself causes computational and storage overheads.

Although the one-to-many encryption mechanism of ABE is an advanced solution compared to traditional approaches, it results in falling back in efficiency when applied into real world scenarios with a large amount of attributes being labelled to keys and ciphertexts if the construction of keys and ciphertexts cannot be optimised. The complexity of access policies that an ABE scheme can support, which we call the expressiveness of an ABE scheme, grows higher to adapt more sophisticated scenarios, and becomes a obstacle to further optimization. More logical and numerical

computations the supported access policy are required, more delicate and complex keys and ciphertexts components have to be constructed, which makes a dilemma between efficiency and expressiveness in ABE research. One of the main objectives of this thesis is to optimize the construction of ciphertexts so the scheme can be more expressive with its efficiency remained.

1.1.2 Inherent Property in Key Management

The encryption process of a public key encryption system requires an encryptor to pick some uniform randomness to hide the message. The encryptor combine this randomness with the public key components, compute a shared secret and encrypt the message with the secret. This shared secret can then be computed by the secret key with other ciphertext components in the decryption process to recover the message. If there are many recipients for one message, the message will then be encrypted several times for each recipient. The flexibility of ABE offers a promising feature to public key encryption that a message only needs to be encrypted once when there are many recipients with different user keys. The nature of this one-to-many feature is that the shared secret can be computed using any user keys as long as the access policy is satisfied.

Take ciphertext-policy attribute-based encryption (CP-ABE) as an example, where the user keys are issued with a set of attributes while the ciphertexts are encrypted with an access policy. The encryption process generates a shared secret for the encryption and then compute other ciphertext components regarding attributes that are possibly needed in the access policy. A user key issued with a set of attributes includes one or many key components for each attribute. If a user private key satisfies the access policy the shared secret can then be computed by combining necessary key and ciphertext components regarding required attributes. Therefore, to decrypt different ciphertexts with one user key different key components will be used. This usage of keys, that the components of a key are separately used when decrypting different ciphertexts, does not lead to security issues and is commonly accepted in most ABE encryption works.

However, this usage of keys, which can be considered as splitting a key into many sub-keys when decrypting different ciphertexts, could give rise to some key management concerns. If new sub-keys are maliciously generated from split key components even if from different private keys, this property could sabotage the basic security requirement of ABE that all user keys must be issued by a trusted authority, usually a private key generator (PKG). One of the main objectives of this thesis is to review this inherent property, establish security model for its abuse and construct ABE schemes that can resist attacks from it.

1.1.3 Adjustable Access Control Management

Data sharing via the Internet has brought many new challenges to data encryption. One of them is that the access control system needs to adapt a more dynamic environment. The access privilege of a user could change from time to time, as well as the intended recipient of a message. If a user has lost his/her access privilege of the shared data or an encryptor needs to share the data to a different set of recipients, the user's access privilege needs to be re-issued or the access control needs to be re-assigned, even with the utility of ABE where the decryption of a ciphertext is decided by an access policy.

For example in a CP-ABE system, the access policy that a ciphertext is encrypted with cannot be changed once the encryption process is completed. As described above, the encryption process in CP-ABE needs to compute the encrypted data as well as other ciphertext components for attributes that could be needed in the access policy. All of these attribute-related ciphertext components are computed associated with the randomness picked during the encryption process. If the access policy has changed and new attributes are included into the access policy it is difficult to compute corresponding ciphertext components without decrypting the ciphertext since the randomness cannot be computed. However, decrypting the ciphertext and re-encrypt the data would result in computation overheads, which is also restricted by many other facts such as network bandwidth, availability of the encryptor, computation capability of the encryptor's device etc.

A mechanism that can adjust the access policy is then highly desired to adapt the dynamic situation. One of the main objectives of this thesis is to construct ABE schemes with adjustable access control management of which the access policy of a ciphertext can be efficiently updated.

1.2 Contributions

The contributions of this thesis are summarised below:

- **Flexible CP-ABE supporting AND-gate and Threshold with Short Ciphertext** We propose a CP-ABE scheme which produces constant-size ciphertexts and supports an AND-gate and threshold access policies. The resulting scheme works for access policies of an AND-gate and a threshold: the sender chooses an ad hoc set S_1 of attributes and another ad hoc set S_2 of attributes with a threshold value t_1, and only users who hold all the attributes in S_1 as well as at least t_1 of the attributes in S_2 can decrypt. Our new scheme is proven secure against selective chosen plaintext attacks in the standard model, under the assumption that the augmented multi-sequence exponent decisional Diffie-Hellman

(aMSE-DDH) problem is hard to solve.

- **Ciphertext-Policy Attribute-Based Encryption with Key-Delegation Abuse Resistance** We propose a CP-ABE scheme in which users cannot illegally generate new private keys of a subset of the users' original sets of attributes. The access structure used in our CP-ABE is constructed by an AND-gate. In our scheme, a ciphertext with the access structure $\mathbb{A}$, which consists of a single AND gate whose input are attributes described by a set of attribute set S, can only be decrypted by a private key of a set of attributes W when $S \subseteq W$.

- **Ciphertext-Policy Attribute Based Encryption Supporting Access Policy Update** We present the notion of Ciphertext-policy Attribute Based Encryption supporting Access Policy Update. We present a new security model to capture these requirements, together with two constructions supporting AND-gate access policy provably secure under augmented assumptions. We also present the proofs of security of our constructions as well as proofs of intractability of augmented assumptions.

- **Applications and Extensions** We propose an application of our CP-ABE scheme against the property of key-delegation abuse in Fog Computing. A traceable CP-ABE scheme, which is a CP-ABE scheme that is equipped with a traitor tracing mechanism, is constructed based on our CP-ABE with key-delegation abuse resistance scheme. We also propose an advanced access policy update mechanism with which the encryptor can preserve certain attributes in an access policy that cannot be revoked in following access policy update.

1.3 Organisation of the Thesis

The rest of the thesis is structured as follows:

Chapter 2 gives a brief review of relevant background material. It starts with mathematical definitions in the area of *Groups*, *Fields*, *Elliptic Curves* and *Pairings*. It then goes through several related cryptographic primitives and complexity assumptions. Backgrounds on security models for attribute-based encryption are also provided in this chapter.

Chapter 3 surveys many previous ABE schemes to present the state-of-the-art with reference to this thesis.

Chapter 4 analyses the dilemma between efficiency and expressiveness in ABE. A solution of a CP-ABE scheme that has constant-size ciphertext and supports the access policy of an AND-gate and an threshold is proposed in this chapter. It is proven secure in the standard security model for CP-ABE against selective chosen

plaintext attacks. The proposed scheme based on the augmented multi-sequence exponent assumption originally appeared in "Flexible Ciphertext-Policy Attribute-Based Encryption Supporting AND-Gate and Threshold with Short Ciphertexts", joint work with Willy Susilo, Yi Mu and Fuchun Guo [JSMG17b].

Chapter 5 examines the property of *key-delegation abuse* in ABE systems. Formal security models for the *key-delegation abuse* problem are defined. A solution of a CP-ABE scheme where user private keys cannot be split or combined to illegally generate new keys is proposed. The proposed scheme based on the Decisional Bilinear Diffie-Hellman problem originally appeared in "Ciphertext-Policy Attribute-Based Encryption with Key-Delegation Abuse Resistance", joint work with Willy Susilo, Yi Mu and Fuchun Guo [JSMG16b].

Chapter 6 studies the issue of access policy update mechanism in ABE systems. A new notion of CP-ABE supporting access policy update is introduced. Formal security models for CP-ABE with attribute addition and revocation against selective chosen plaintext attacks are defined. Solutions of CP-ABE schemes that has access policy update mechanisms, regarding attribute addition and revocation, are proposed. The proposed schemes based on two augmented multi-sequence exponent assumptions originally appeared in "Ciphertext-Policy Attribute-Based Encryption Supporting Access policy Update", joint work with Willy Susilo, Yi Mu and Fuchun Guo [JSMG16a].

Chapter 7 presents applications of proposed and new CP-ABE schemes in specific scenarios. It starts with application of CP-ABE with key-delegation abuse resistance for traceable CP-ABE in Fog Computing. It then gives new solutions for CP-ABE with access policy update mechanism in the scenario where certain attributes need to be preserved. The proposed scheme with tracing functionality originally appeared in "Ciphertext-Policy Attribute-Based Encryption against Key-Delegation Abuse in Fog Computing", joint work with Willy Susilo, Yi Mu and Fuchun Guo [JSMG18]. The other proposed scheme support access policy update with preserved attributes originally appeared in "Ciphertext-Policy Attribute-Based Encryption Supporting Access Policy Update and Its Extension with Preserved Attributes", joint work with Willy Susilo, Yi Mu and Fuchun Guo [JSMG17a].

Chapter 8 concludes the thesis and discusses some possible directions of future work.

Chapter 2

Preliminaries

We present related mathematical background and cryptographic primitives that are used in this thesis.

2.1 Mathematical Background

Related mathematical background are presented in this subsection.

2.1.1 Fields and Groups

Definition 2.1. *A group is a set with an operation* $(\mathbb{G}, \circ)$ *such that*

- $(\mathbb{G}, \circ)$ *is closed:*
$$\forall g, h \in \mathbb{G} : g \circ h \in \mathbb{G},$$
- $(\mathbb{G}, \circ)$ *has an identity:*
$$\forall g \in \mathbb{G} : \exists e \in \mathbb{G}, g \circ e = e \circ g = g,$$
- *the operation* $\circ$ *is associative:*
$$\forall g, h, u \in \mathbb{G} : (g \circ h) \circ u = g \circ (h \circ u),$$
- *every element in* $\mathbb{G}$ *has an inverse:*
$$\forall g \in \mathbb{G} : \exists h \in \mathbb{G}, g \circ h = h \circ g = e.$$

If $\mathbb{G}$ *is finite and has* n *elements, then we call* n *the order of* $\mathbb{G}$ *and we write* $\#\mathbb{G} = n$*. If* $\mathbb{G}$ *is infinite, we say that* $\mathbb{G}$ *has infinite order and we write* $\#\mathbb{G} = \infty$*.*

Definition 2.2. *An Abelian group is a set with an operation* $(\mathbb{G}, \circ)$ *such that*

- $(\mathbb{G}, \circ)$ *is a group,*
- *the operation* $\circ$ *is commutative:*
$$\forall g, h \in \mathbb{G} : g \circ h = h \circ g.$$

Definition 2.3. *A cyclic group is a set with an operation* $(\mathbb{G}, \circ)$ *such that*

- $(\mathbb{G}, \circ)$ *is an abelian group,*
- $(\mathbb{G}, \circ)$ *has a special element, called generator, from which every other element can be obtained by repeated application of the group operation:*

$$\forall h \in \mathbb{G} : \exists g \in \mathbb{G}, x \in \mathbb{N}, h = \underbrace{g \circ g \circ \cdots \circ g}_{x-1 \text{ times of operation } \circ}.$$

If the operation $\circ$ *is multiplication then every element of* $\mathbb{G}$ *can be written as*

$$h = g^x$$

, whilst if $\circ$ *is addition then every element* h *of* $\mathbb{G}$ *can be written as*

$$h = x \cdot g.$$

Definition 2.4. *A field is a set of two operations* $(\mathbb{F}, \circ, \bullet)$ *such that*

- $(\mathbb{F}, \circ)$ *is an abelian group with identity denoted by* e*,*
- $(\mathbb{F} \setminus \{e\}, \bullet)$ *is an abelian group,*
- $(\mathbb{F}, \circ, \bullet)$ *satisfies the distributive law:*

$$\forall g, h, u \in \mathbb{F} : (g \circ h) \bullet u = (g \bullet u) \circ (g \bullet h).$$

Definition 2.5. *A finite field is a set of two operations* $(\mathbb{F}, \circ, \bullet)$ *such that*

- $(\mathbb{F}, \circ, \bullet)$ *is a field,*
- $(\mathbb{F}, \circ, \bullet)$ *has finite group order.*

2.1.2 Elliptic Curves and Pairing

Miller [Mil85] introduced Elliptic Curves for constructing public key cryptographic systems.

Definition 2.6. *Let* K *be a finite field* $\mathbb{F}_q$ *where* $q = p^n$ *for a prime* $p > 3$ *and an integer* $n \geq 1$*. An elliptic curve is a plain curve over a finite field which consists of the points satisfying the equation* $Y^2 = X^3 + aX + b$ *where* $a, b \in K$*, along with a distinguished point at infinity* ∞*, denoted by* $\mathcal{O}$*. It has the following property:*

- *Coefficients* $a, b \in K$ *satisfying the discriminant* $\triangle = -16(4a^3 + 27 \cdot b^2) \neq 0$*;*

Definition 2.7 (Bilinear Map)**.** *Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ be three cyclic groups of the same order. A bilinear map $e(\cdot,\cdot)$is a mapping from the product $\mathbb{G}_1 \times \mathbb{G}_2$ into $\mathbb{G}_T$ such that*

- *$e(\cdot,\cdot)$ is bilinear:*

$$\forall g \in \mathbb{G}_1, h \in \mathbb{G}_2, a, b \in \mathbb{Z} : e(g^a, h^b) = e(g,h)^{ab},$$

- *$e(\cdot,\cdot)$ is non-degenerate:*

$$\forall g \in \mathbb{G}_1, h \in \mathbb{G}_2 : e(g,h) \neq 1,$$

- *$e(\cdot,\cdot)$ is efficiently computable.*

Remark 2.8. A bilinear map group system is a tuple $\mathbb{S} = (N = |\mathbb{G}_1|, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(\cdot,\cdot))$ where N is usually a prime number, composed of objects as described above.

Definition 2.9 (Generic Bilinear Group Model)**.** *The generic bilinear group model of a bilinear map system $\mathbb{S}$ is a tuple $(\psi_1, \psi_2, \psi_T, \sigma_1, \sigma_2, \sigma_T, \sigma_e)$ such that*

- *ψ_1 is an injective random mapping from $\mathbb{G}_1$ to $\{0,1\}^m$ where $m > 3\log(p)$.*
- *ψ_2 is an injective random mapping from $\mathbb{G}_2$ to $\{0,1\}^m$ where $m > 3\log(p)$.*
- *ψ_T is an injective random mapping from $\mathbb{G}_T$ to $\{0,1\}^m$ where $m > 3\log(p)$.*
- *σ_1 is an oracle that takes input $\psi_1(x)$ and $\psi_1(y)$ and outputs $\psi_1(xy)$ for all $x, y \in \mathbb{G}_1$.*
- *σ_2 is an oracle that takes input $\psi_2(x)$ and $\psi_2(y)$ and outputs $\psi_2(xy)$ for all $x, y \in \mathbb{G}_2$.*
- *σ_T is an oracle that takes input $\psi_T(x)$ and $\psi_T(y)$ and outputs $\psi_T(xy)$ for all $x, y \in \mathbb{G}_T$.*
- *σ_e is an oracle that takes input $\psi_1(x)$ and $\psi_2(y)$ and outputs $\psi_T(e(x,y))$ for all $x \in \mathbb{G}_1, y \in \mathbb{G}_2$.*

2.2 Cryptographic Primitives

Related cryptographic primitives are reviewed in this section.

2.2.1 Hash Functions

Definition 2.10. *A cryptographic hash function is a function which takes input a message of an arbitrary length bit string and outputs a hash value of a fixed length bit string* $H : \{0,1\}^* \to \{0,1\}^l$ *that satisfies the following three properties [RS04] :*

Preimage Resistant: *It should be hard to find a message with a given hash value.*

Collision Resistant: *It should be hard to find two messages with the same hash value.*

Second Preimage Resistant: *Given one message it should be hard to find another message with the same hash value.*

2.2.2 Secret Sharing

2.2.2.1 Attribute and Attribute Universe

An *attribute* is denoted by A. Let $\{A_1, \ldots, A_n\}$ be the set of all attributes, which is then called *attribute universe* denoted by $\mathcal{P}$ with size $n = |\mathcal{P}|$.

2.2.2.2 Access Structure

Definition 2.11 (Access Structure [B96])**.** *Consider a set of parties* $\mathcal{Q} = \{Q_1, Q_2, \ldots, Q_n\}$*. A collection* $\mathbb{A} \subseteq 2^{\mathcal{Q}}$ *is said to be monotone if, for all* W*,* W'*, if* $W \in \mathbb{A}$ *and* $W \subseteq W'$*, then* $W' \in \mathbb{A}$*. An access structure (resp., monotonic access structure) is a collection (resp., monotone collection)* $\mathbb{A} \subseteq 2^{\mathcal{Q}} \setminus \emptyset$*. The sets in* $\mathbb{A}$ *are called the authorised sets, and the sets not in* $\mathbb{A}$ *are called the unauthorised sets. Notation* $W \models \mathbb{A}$ *is used to represent the fact that* $W \in \mathbb{A}$*, and the case of* $W \notin \mathbb{A}$ *is denoted by* $W \not\models \mathbb{A}$*.*

Definition 2.12 (AND-gate Access Structure)**.** *An access structure* $\mathbb{A}$ *is said to be an AND-gate access structure if there exists a set of parties* $S_1 \subset \mathcal{Q}$ *such that* $W \in \mathbb{A}$ *if and only if* $S_1 \subseteq W \subseteq \mathcal{Q}$*.*

Definition 2.13 (Threshold Access Structure)**.** *An access structure* $\mathbb{A}$ *is said to be a threshold access structure if there exists a set of parties* $S_1 \subset \mathcal{Q}$ *with some positive integer* t_1 *such that* $W \in \mathbb{A}$ *if and only if* $|W \cap S_1| \geq t_1$ *for* $W \subseteq \mathcal{Q}$*.*

Definition 2.14 (AND-gate and Threshold Access Structure)**.** *An access structure* $\mathbb{A}$ *is said to be an AND-gate and threshold access structure if there exists two disjoint sets of parties* $S_1, S_2 \subset \mathcal{Q}$ *with some positive integer* t_1 *such that* $W \in \mathbb{A}$ *if and only if* $|W \cap S_1| \geq t_1$ *and* $S_2 \subseteq W$*.*

Definition 2.15 (Access Tree [GPSW06]). *Let $\mathcal{T}$ be a tree where each non-leaf node represents a threshold gate described by its children and a threshold value, which is satisfied if the number of satisfied children nodes is at least the threshold value, and each leaf node represents an AND-gate of a single party from $\mathcal{Q}$. Hence $\mathcal{T}$ is said to be satisfied by a set W of parties if and only if parties of the AND-gates of leaf nodes needed to satisfy the threshold gate of the root of T are included in W. An access structure $\mathbb{A}$ is said to be an access tree access structure if there exists an access tree $\mathcal{T}$ involving several parties in its leaf nodes such that $W \in \mathbb{A}$ if and only if W satisfies $\mathcal{T}$.*

Definition 2.16 (Linear Secret-Sharing Scheme (LSSS) [B96]). *A secret-sharing scheme Π over a set of parties $\mathcal{Q}$ is called linear (over $\mathbb{Z}_p$) if*

- *The shares for each party form a vector over $\mathbb{Z}_p$.*
- *There exists a matrix M_Π with l rows and n columns called the share-generating matrix for Π. For all $i = 1, \ldots, l$, the i'th row of M_Π we let the function ρ defined the party labelling row i as $\rho(i)$. When we consider the column vector $v = (s, r_2, \ldots, r_n)$, where $s \in \mathbb{Z}_p$ is the secret to be shared, and $r_2, \ldots, r_n \in \mathbb{Z}_p$ are randomly chosen, then Mv is the vector of l shares of the secret s according to Π. The share $(Mv)_i$ belongs to party $\rho(i)$.*

It is shown in [B96] that every linear secret sharing-scheme according to the above definition also enjoys the linear reconstruction property, defined as follows: Suppose that Π is an LSSS for the access structure $\mathbb{A}$. Let $W \in A$ be any authorised set, and let $I \subset \{1, 2, \ldots, l\}$ be defined as $I = \{i : \rho(i) \in W\}$. Then, there exist constants $\{\omega_i \in \mathbb{Z}_p\}_{i \in I}$ such that, if $\{\lambda_i\}$ are valid shares of any secret s according to Π, then $\sum_{i \in I} \omega_i \lambda_i = s$. Furthermore, it is shown in [B96] that these constants ω_i can be found in time polynomial in the size of the share-generating matrix M_Π.

2.2.3 Definitions in Functional Encryption

We begin by describing the syntactic definition of Functional Encryption for a functionality F. The functionality F describes the functions of a plaintext that can be learned from the ciphertext. More precisely, a functionality is defined as follows [BSW11].

Definition 2.17. *A functionality F defined over $(\mathcal{K}, \mathcal{M})$ is a function $F : \mathcal{K} \times \mathcal{M} \to \{0,1\}^*$ described as a (deterministic) Turing Machine. The set $\mathcal{K}$ is called the key space and the set $\mathcal{M}$ is called the plaintext space. We require that the key space $\mathcal{K}$ contain a special key called the empty key denoted ϵ.*

A functional encryption scheme for the functionality F enables one to evaluate $F(k, M)$ given the encryption of $M \in \mathcal{M}$ and a secret key sk_k for $k \in \mathcal{K}$. The algorithm for evaluation $F(k, M)$ using sk_k is called decrypt. More precisely, a functional encryption scheme is defined as follows.

Definition 2.18. *A functional encryption scheme for a functionality F defined over (K, X) is a tuple of four probabilistic polynomial time algorithms* (Setup, Enc, KeyGen, Dec) *satisfying the following correctness condition for all $k \in \mathcal{K}$ and $M \in \mathcal{M}$ [BSW11]:*

Setup(1^λ)**.** This is a randomised algorithm performed by an authority in order to create a new FE scheme. The setup algorithm takes no input other than the implicit security parameter λ. It outputs the public parameters params and a master secret key msk.

Enc(params, M)**.** The encryption algorithm takes in the public parameters params, the plaintext $M \in \mathcal{M}$. It outputs a ciphertext CT.

KeyGen(msk, k)**.** The key generation algorithm takes as input the master secret msk and $k \in K$. It outputs a private key sk_k associated with k. This algorithm must be run by the trusted authority, usually a private key generator (PKG).

Dec(params, CT, sk_k)**.** The decryption algorithm takes as input the public parameters params, a ciphertext CT, and a private key sk_k. It outputs y as the result.

We require that $y = F(k, M)$ with probability 1.

2.2.3.1 KP-ABE Definition

A key-policy attribute-based encryption system consists of four algorithms: Setup, Enc, KeyGen, and Dec [GPSW06].

Setup$(1^\lambda, \mathcal{P})$**.** The setup algorithm takes in the security parameters λ and the attribute universe $\mathcal{P}$. It outputs the public parameters params and a master secret key msk.

Encrypt(params, M, W)**.** The encryption algorithm takes in the public parameters params, the message M, and a set of attributes W. It outputs a ciphertext CT such that only users with whose private keys associated with access policies that can be satisfied by the set of attributes W can decrypt M. We assume that the ciphertext implicitly contains W.

KeyGen(msk, $\mathbb{A}$). The key generation algorithm, which is run by a PKG, takes as input the master secret msk and an access structure $\mathbb{A}$. It outputs a private key sk associated with $\mathbb{A}$.

Decrypt(params, CT, sk). The decryption algorithm takes as input the public parameters params, a ciphertext CT, which contains a set of attributes W, and a private key sk, which is a private key for an access structure $\mathbb{A}$. If the attribute set W satisfies the access structure $\mathbb{A}$ then the algorithm will decrypt the ciphertext and return a message M.

2.2.3.2 CP-ABE Definition

A ciphertext-policy attribute-based encryption encryption system consists of four algorithms: Setup, Enc, KeyGen, and Dec [BSW07].

Setup($1^\lambda, \mathcal{P}$). The setup algorithm takes in the security parameters λ and the attribute universe $\mathcal{P}$. It outputs the public parameters params and a master secret key msk.

Encrypt(params, M, $\mathbb{A}$). The encryption algorithm takes in the public parameters params, the message M, and an access structure $\mathbb{A}$ over the universe of attributes. It outputs a ciphertext CT such that only users with whose private keys associated with attribute sets which satisfy the access structure $\mathbb{A}$ can decrypt M. We assume that the ciphertext implicitly contains $\mathbb{A}$.

KeyGen(msk, W). The key generation algorithm, which is run by a PKG, takes as input the master secret msk and a set of attributes W. It outputs a private key sk associated with W.

Decrypt(params, CT, sk). The decryption algorithm takes as input the public parameters params, a ciphertext CT, which contains an access structure $\mathbb{A}$, and a private key sk, which is a private key for a set of attributes W. If the attribute set W satisfies the access structure $\mathbb{A}$ then the algorithm will decrypt the ciphertext and return a message M.

2.3 Security Models for Attribute-based Encryption

This subsection gives detailed security models for KP-ABE and CP-ABE.

2.3.1 IND-CPA Security Models for Key-Policy Attribute-Based Encryption

We now give the security definition for KP-ABE system – Indistinguishability under chosen plaintext attacks (IND-CPA). This is described by a security game between a challenger and an adversary for a security parameter $\lambda \in \mathbb{N}$. The game proceeds as follows:

Setup The challenger runs the Setup algorithm and gives the public parameters params to the adversary.

Phase 1 The adversary queries the challenger for private keys corresponding to access structures $\mathbb{A}_1, \ldots, \mathbb{A}_{q_1}$.

Challenge The adversary declares a challenge set of attributes W^* and two equal length messages M_0 and M_1. The challenger flips a random coin $\beta \in \{0, 1\}$, and encrypts M_β with W^*, producing CT^*. It gives CT^* to the adversary.

Phase 2 The adversary queries the challenger for private keys corresponding to sets of attributes $\mathbb{A}_{q_1+1}, \ldots, \mathbb{A}_q$ with the restriction that none of these can be satisfied by the set of attributes W^*.

Guess The adversary outputs a guess β' for β.

The advantage of an adversary in winning this game is defined to be

$$\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathcal{A},\mathsf{KP\text{-}ABE}} = |\Pr[\beta' = \beta] - \frac{1}{2}|.$$

Definition 2.19. *A key-policy attribute-based encryption system is chosen-plaintext attacks secure if all polynomial time adversaries have at most a negligible advantage in this security game.*

2.3.2 IND-sCPA Security Models for Key-Policy Attribute-Based Encryption

We now give the security definition of Indistinguishability under selective chosen plaintext attacks (IND-sCPA) for KP-ABE system. This is described by a security game between a challenger and an adversary for a security parameter $\lambda \in \mathbb{N}$. The game proceeds as follows:

Init The challenger defines an attribute universe $\mathcal{P}$ of size n and gives it to the adversary $\mathcal{A}$. $\mathcal{A}$ chooses a challenge set of attributes W^* and gives it to the challenger.

Setup The challenger runs the Setup algorithm and gives the public parameters params to the adversary.

Phase 1 The adversary queries the challenger for private keys corresponding to access structure $\mathbb{A}_1, \ldots, \mathbb{A}_{q_1}$ with the restriction that none of these can be satisfied by the set of attributes W^*.

Challenge The adversary declares two equal length messages M_0 and M_1. The challenger flips a random coin $\beta \in \{0, 1\}$, and encrypts M_β with W^*, producing CT^*. It gives CT^* to the adversary.

Phase 2 The adversary queries the challenger for private keys corresponding to access structure $\mathbb{A}_{q_1+1}, \ldots, \mathbb{A}_q$ with the same restriction that none of these can be satisfied by the set of attributes W^*.

Guess The adversary outputs a guess β' for β.

The advantage of an adversary in winning this game is defined to be

$$\mathsf{Adv}^{\mathsf{IND\text{-}sCPA}}_{\mathcal{A},\mathsf{KP\text{-}ABE}} = |\Pr[\beta' = \beta] - \frac{1}{2}|.$$

Definition 2.20. *A key-policy attribute-based encryption system is selective chosen-plaintext attacks secure if all polynomial time adversaries have at most a negligible advantage in this security game.*

2.3.3 IND-CPA Security Models for Ciphertext-Policy Attribute-Based Encryption

We now give the security definition of IND-CPA for CP-ABE system. This is described by a security game between a challenger and an adversary for a security parameter $\lambda \in \mathbb{N}$. The game proceeds as follows:

Setup The challenger runs the Setup algorithm and gives the public parameters params to the adversary.

Phase 1 The adversary queries the challenger for private keys corresponding to sets of attributes $W_1, \ldots, W_{q_1}$.

Challenge The adversary declares a challenge access structure $\mathbb{A}^*$ and two equal length messages M_0 and M_1. The challenger flips a random coin $\beta \in \{0, 1\}$, and encrypts M_β with $\mathbb{A}^*$, producing CT^*. It gives CT^* to the adversary.

Phase 2 The adversary queries the challenger for private keys corresponding to sets of attributes $W_{q_1+1}, \ldots, W_q$ with the restriction that none of these satisfies the access policy $\mathbb{A}^*$.

Guess The adversary outputs a guess β' for β.

The advantage of an adversary in winning this game is defined to be

$$\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathcal{A},\mathsf{CP\text{-}ABE}} = |\Pr[\beta' = \beta] - \frac{1}{2}|.$$

Definition 2.21. *A ciphertext-policy attribute-based encryption system is chosen-plaintext attacks secure if all polynomial time adversaries have at most a negligible advantage in this security game.*

2.3.4 IND-sCPA Security Models for Ciphertext-Policy Attribute-Based Encryption

We now give the security definition of IND-sCPA for CP-ABE system. This is described by a security game between a challenger and an adversary for a security parameter $\lambda \in \mathbb{N}$. The game proceeds as follows:

Init The challenger defines an attribute universe $\mathcal{P}$ of size n and gives it to the adversary $\mathcal{A}$. $\mathcal{A}$ chooses a challenge access structure $\mathbb{A}^*$ and gives it to the challenger.

Setup The challenger runs the Setup algorithm and gives the public parameters params to the adversary.

Phase 1 The adversary queries the challenger for private keys corresponding to sets of attributes $W_1, \ldots, W_{q_1}$ with the restriction that none of these satisfies the access policy $\mathbb{A}^*$.

Challenge The adversary declares two equal length messages M_0 and M_1. The challenger flips a random coin $\beta \in \{0, 1\}$, and encrypts M_β with $\mathbb{A}^*$, producing CT^*. It gives CT^* to the adversary.

Phase 2 The adversary queries the challenger for private keys corresponding to sets of attributes $W_{q_1+1}, \ldots, W_q$ with the same restriction that none of these satisfies the access policy $\mathbb{A}^*$.

Guess The adversary outputs a guess β' for β.

The advantage of an adversary in winning this game is defined to be

$$\mathsf{Adv}^{\mathsf{IND\text{-}sCPA}}_{\mathcal{A},\mathsf{CP\text{-}ABE}} = |\Pr[\beta' = \beta] - \frac{1}{2}|.$$

Definition 2.22. *A ciphertext-policy attribute-based encryption system is selective chosen-plaintext attacks secure if all polynomial time adversaries have at most a negligible advantage in this security game.*

2.4 Complexity Assumptions

Complexity assumptions that will be used in this thesis are presented in section. Let $\mathbb{S} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(\cdot,\cdot))$ be a bilinear group system, g_1 be an arbitrary generator of $\mathbb{G}_1$ and g_2 be an arbitrary generator of $\mathbb{G}_2$.

2.4.1 Basic Assumptions

Definition 2.23 (Bilinear Diffie-Hellman Assumption [BF01a])**.** *Suppose a challenger chooses $a, b, c, z \in \mathbb{Z}_p$ at random. The Bilinear Diffie-Hellman assumption is that no polynomial-time adversary is to be able to compute $e(g_1, g_2)^{abc}$ given the tuple $(A = g_1^a, B = g_1^b, C = g_1^c)$ with more than a negligible advantage where the probability is taken over the random choice of the generator g_1 and g_2.*

Definition 2.24 (Decisional Bilinear Diffie-Hellman (DBDH) Assumption [GPSW06])**.** *Suppose a challenger chooses $a, b, c, z \in \mathbb{Z}_p$ at random. The Decisional Bilinear Diffie-Hellman assumption is that no polynomial-time adversary is to be able to distinguish the tuple $(A = g_1^a, B = g_1^b, C = g_1^c, Z = e(g_1, g_2)^{abc})$ from the tuple $A = g_1^a, B = g_1^b, C = g_1^c, Z = e(g_1, g_2)^z)$ with more than a negligible advantage where the probability is taken over the random choice of the generator g_1 and g_2.*

Definition 2.25 (Decision Linear (D-linear) Assumption [NYO09])**.** *Suppose a challenger chooses $a, b, c, d, z \in \mathbb{Z}_p$ at random. The Decision Linear assumption is that no polynomial-time adversary is to be able to distinguish the tuple $(g^a, g^b, g^{ac}, g^{bd}, g^{c+d})$ from the tuple $(g^a, g^b, g^{ac}, g^{bd}, g^z)$ with more than a negligible advantage where the probability is taken over the random choice of the generator g.*

Definition 2.26 (Subgroup Decision Problem for 3 Primes (3P-SDP) Assumption [LOS+10])**.** *Suppose a challenger chooses $a, z_1 \in \mathbb{Z}_{p_1}, z_2 \in \mathbb{Z}_{p_1 p_2}, b \in \mathbb{Z}_{p3}$ at random. The Subgroup Decision Problem for 3 Primes is that no polynomial-time adversary is to be able to distinguish the tuple $(g_1^a, g_3^b, g_1^{z_1})$ from the tuple $(g_1^a, g_3^b, (g_1 g_2)^{z_2})$ with more than a negligible advantage where the probability is taken over the random choice of the generators g_1, g_2, g_3 of subgroups $\mathbb{G}_{p_1}, \mathbb{G}_{p_2}, \mathbb{G}_{p_3}$, respectively, from a composite order group $\mathbb{G}$ with $|\mathbb{G}| = p_1 p_2 p_3$.*

2.4.2 General Diffie-Hellman Exponent Problem

Let $\mathbb{S}_S = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(\cdot,\cdot))$ be a symmetric bilinear group such that $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$. Let $g \in \mathbb{G}$ be a generator of $\mathbb{G}$, and set $g_T = e(g,g) \in \mathbb{G}_T$. Let s, n be two positive integers and $P, Q \in \mathbb{F}_p[X_1, \ldots, X_n]^s$ be two lists containing s n-variate polynomials over $\mathbb{F}_p$. Thus, P and Q can be written as $P = (p_1, p_2, \ldots, p_s)$ and $Q = (q_1, q_2, \ldots, q_s)$, and impose that $p_1 = q_1 = 1$. For a set Ω, a function $h : \mathbb{F}_p \to \Omega$ and vector $(x_1, ..., x_n) \in \mathbb{F}_p^n$, the notation $h(P(x_1, \ldots, x_n))$ stands for $(h(p_1(x_1, \ldots, x_n)),$ $\ldots,$ $h(p_s(x_1, \ldots, x_n))) \in \Omega^s$. We use a similar notation for the s-tuple Q. Let $f \in \mathbb{F}_p[X_1, ..., X_n]$. The computational and decisional (P, Q, f)-General Diffie-Hellman Exponent (GDHE) Problems are defined as follows.

Definition 2.27 ((P, Q, f)-GDHE Problem [BBG05])**.** *Given the tuple*

$$H(x_1, ..., x_n) = \left(g^{P(x_1,...,x_n)}, g_T^{Q(x_1,...,x_n)}\right) \in \mathbb{G}^s \times \mathbb{G}_T^s,$$

compute $g^{f(x_1,...,x_n)}$.

Definition 2.28 (Decisional (P, Q, f)-GDHE Problem [BBG05])**.** *Given* $H(x_1, ..., x_n)$ $\in \mathbb{G}^s \times \mathbb{G}_T^s$ *as above, and* $T \in \mathbb{G}_T$ *which is picked at random, decide whether* $T = g^{f(x_1,...,x_n)}$.

2.4.2.1 Complexity Lower Bound of Decisional (P, Q, f)-GDHE Problem in Generic Bilinear Groups

To state the lower bound on the decisional (P, Q, f)-GDHE Problem, the definition of the dependencies between a polynomial $f \in \mathbb{F}_p[X_1, \ldots, X_n]$ and the sets (P, Q) of s-tuples of n-variate polynomials over $\mathbb{F}_p$ is needed [BBG05].

Definition 2.29. *Let* $P = (p_1, p_2, \ldots, p_s)$, $Q = (q_1, q_2, \ldots, q_s) \in \mathbb{F}_p[X_1, \ldots, X_n]^s$ *be two* s*-tuples of* n*-variate polynomials over* $\mathbb{F}_p$ *where* $p_1 = q_1 = 1$. *A polynomial* $f \in \mathbb{F}_p[X_1, \ldots, X_n]$ *is dependent on* (P, Q)*, which we denote by* $f \in \langle P, Q \rangle$*, when there exists a linear decomposition* $f = \sum_{1 \le i,j \le s} a_{i,j} \cdot p_i \cdot p_j + \sum_{1 \le i \le s} b_i \cdot q_i$*, where* $a_{i,j}, b_i \in \mathbb{Z}_p$.

For a polynomial $f \in \mathbb{F}_p[X_1, \ldots, X_n]$, we let d_f denote the total degree of f. For a set $P \subset \mathbb{F}_p[X_1, \ldots, X_n]^s$ we let $d_P = \max\{d_f | f \in P\}$. We then state the following lower bound in the framework of the generic group model. Let (ψ_1, ψ_2, ψ_T, σ_1, σ_2, σ_T, σ_e) be the generic bilinear group model of a symmetric bilinear group system $\mathbb{S}_S = (p, \mathbb{G}, \mathbb{G}_T, e(\cdot,\cdot))$. Thus, $\psi_1 = \psi_2 = \psi$ for random encoding group elements from $\mathbb{G}$ to $\{0,1\}^m$ where $m > \log(p)$ and $\sigma_1 = \sigma_2 = \sigma$ as the oracle that computes group operation in $\mathbb{G}$.

Theorem 2.30 (Complexity Lower Bound of Decisional (P, Q, f)-GDHE Problem [BBG05])**.** *Let $P, Q \in \mathbb{F}_p[X_1, \ldots, X_n]^s$ be two s-tuples of n-variate polynomials over $\mathbb{F}_p$ and let $f \in \mathbb{F}_p[X_1, \ldots, X_n]$. Let $d = \max(2d_P, d_Q, d_f)$. Let $(\psi, \psi_T, \sigma, \sigma_T, \sigma_e)$ be defined as above. If $f \notin \langle P, Q \rangle$ then for any $\mathcal{A}$ that makes a total of at most q queries to the oracles its advantage in solving Decisional (P, Q, f)-GDHE Problem is bonded as*

$$\mathsf{Adv}_{\mathcal{A}}^{\text{Decisional}(P,Q,f)-\text{GDHE}} \leq \frac{(q + 2s + 2)^2 \cdot d}{2p}$$

Chapter 3

Previous Attribute-Based Encryption Schemes

Fuzzy IBE [SW05] was the first attribute-based encryption scheme: given a ciphertext CT encrypted with a set of attributes S, one can decrypt it only if the set of attributes W with which his/her private key is associated has more than t attributes that also belong to S, where t is a threshold value. Fuzzy IBE was a natural extension of previous IBE schemes that requires identical matching of identities from private keys and ciphertexts in decryption. Although the error-tolerance property allowed an interesting application of IBE using biometric identities, the latent possibilities of the various descriptive attributes drew the one-to-many cryptographic primitive – attribute-based encryption. However, fuzzy IBE could only support decryption when a "threshold" policy with a prefixed threshold value is satisfied. The need of flexible access control policies that can be supported by attributed-based encryption urged the pursuit of efficient ABE schemes with more expressiveness.

More and richer types of ABE schemes were proposed afterwards. Most of them can be divided into two main categories: Key-policy ABE schemes and Ciphertext-policy ABE schemes. In Fuzzy IBE, the requirement of decryption is based on how many attributes both the sets of attributes associated with a private key and a ciphertext have. Thus, the protection strategy is not clear since the forced requirement can be seen as have been put in private keys, so that only ciphertexts with sets of attributes that can satisfy the requirement can be decrypted, or vice versa. In order to achieve more expressive access control, the deployment of protection strategy is then explicitly assigned to private keys or ciphertexts. Besides the categorization of protection strategy deployment, ABE schemes can also be classified by different supplemental functionalities that emerged and motivated in practical applications. These functionalities include Revocation mechanism, Accountability and so on.

In this chapter we survey important previous ABE schemes according to the classifications of basic ABE schemes of KP-ABE and CP-ABE, and ABE schemes supporting supplemental functionalities.

3.1 Previous Basic Attribute-Based Encryption Schemes

Basic ABE schemes resolve the problem of data confidentiality in its one-to-many encryption scenario, tackle the core issue of collusion attacks and smooth the dilemma between computation overhead and access control expressiveness. Collusion attacks belong to a special type of attacks that users collude their private keys and try to decrypt ciphertexts beyond their total access privileges. It is a fundamental security requirement for ABE schemes to resist collusion attacks.

Most of previous basic ABE schemes can be categorised as KP-ABE schemes or CP-ABE schemes according to where the access control protection strategy is deployed. If the protection strategy is deployed at private keys, the ABE scheme is called key-policy ABE scheme where a private key for a user is generated assocaited with an access policy while a ciphertext that is encrypted with a set of attributes satisfying the access policy can be decrypted. If the protection strategy is deployed at ciphertexts, the ABE scheme is called ciphertext-policy ABE scheme where a ciphertext on a message is encrypted with an access policy while a private key for a user that can decrypt needs to be associated with a set of attributes satisfying the access policy. A brief examination to these schemes will be given in this section.

3.1.1 Key-Policy Attribute-Based Encryption

Goyal et al. [GPSW06] proposed the first key-policy attribute-based encryption scheme in 2006. KP-ABE is an altered form of Fuzzy IBE. It encrypts messages with sets of attributes and generates users' private keys based on expressive access policies. If attributes of the encrypted data satisfies the access structure in user's private key sk, an user can recover the message through the decrypt algorithm.

In KP-ABE, the KeyGen algorithm is different from Fuzzy IBE as it generates user private keys according to the access structure. Take Goyal et al.'s work [GPSW06] as an example of a KP-ABE scheme supporting access trees. In its KeyGen algorithm, it adopts secret sharing and chooses a polynomial q_x for Node x in access tree structure such that $q_x(0) = q_{parent(x)}(index(x))$, where $parent(x)$ is x's parent node and $index(x)$ is the index number of node x that is given by x's parent node, in a top-down manner from the root node r. Then as $q_r(0)$ is set equal to the master key y, the master key y is distributed among the user's private key components which are corresponding to the leaf nodes that represents attribute. In the Dec algorithm, it uses attributes of encrypted data to run decryptnode function in the decryption algorithm, which inputs encrypted data, user's private key, and nodes of the access structure in user's private key; adopts bottom-up manner in the

access tree structure and decrypt the ciphertext recursively. Finally, it will get a bilinear formula and use polynomial interpolation to get the message.

The scheme consists of four algorithms of the KP-ABE scheme. It will be described as follows.

GSPW06 KP-ABE Scheme [GPSW06]

$\mathsf{Setup}(\lambda)$: The authority chooses several uniformly random numbers $t_1, \ldots, t_n, y$ from $\mathbb{Z}_p$. The published public parameters are $\mathsf{params} = \big(T_1 = g^{t_1}, \ldots, T_n = g^{t_n}, Y = e(g,g)^y\big)$. The kept master key is $\mathsf{msk} = (t_1, \ldots, t_n, y)$.

$\mathsf{KeyGen}(\mathsf{params}, \mathsf{msk}, \mathbb{A})$: The authority generates private key components for each leaf node x in the access tree structure $\mathbb{A}$. The private key components are $D_x = g^{\frac{q_x(0)}{t_i}}$, where i is equal to a leaf node attribute in the access tree structure. These components will be merged into the user's private key sk, and be sent to an user.

$\mathsf{Enc}(M, S, \mathsf{params})$ Encryptor chooses a random number s from $\mathbb{Z}_p$ and encrypts a message $M \in \mathbb{G}_2$ with a set of attributes A_C, and then he generates the ciphertext as $CT = (S, E = MY^s = e(g,g)^{ys}, \{E_i = g^{t_i s}\}_{\forall i \in S})$.

$\mathsf{Dec}(CT, sk)$ This algorithm inputs the encrypted data, user's private key, and nodes of the access structure in user's private key. It deploys a $\mathsf{decryptnode}(sk, CT, x)$ function for bilinear map computation. If i is equal to the leaf node x attribute, $\mathsf{decryptnode}(sk, CT, x)$ outputs $e(D_x, E_i) = e(g,g)^{s \cdot q_x(0)}$. If node x is a leaf node but there is no $i \in A_C$ matching node x's attribute, the $\mathsf{decryptnode}(sk, CT, x)$ outputs invalid. If node x is not a leaf node, it will call itself multiple times $\mathsf{decryptnode}(sk, CT, z)$ for all children nodes z of node x, and use lagrange coefficient to compute $e(g,g)^{s \cdot q_x(0)}$. Finally, the decryption algorithm obtains $e(g,g)^{ys} = Y^s$ by running $\mathsf{decryptnode}(sk, CT, r)$ at root node, if and only if the encrypted data satisfies the access structure of private key. And the message $M = \frac{E}{Y^s}$ can be obtained.

In 2007, a KP-ABE scheme supporting non-monotonic access structure is proposed by Ostrovsky et al. [OSW07] where there are two values for each attribute as positive and negative. Compared with the "GSPW06" KP-ABE scheme, Ostrovsky et al.'s work can express more complex access policies and offer more delicate key management. A trade-off for the advanced expressiveness is that the scheme doubles the size of ciphertexts and private keys adding overheads for both encryption and decryption. Lewko et al. [LSW10] then improved Ostrovsky et al.'s basic construction with new techniques and designed the most efficient non-monotonic KP-ABE scheme. They also achieved user revocation in their improved scheme.

Most of the above KP-ABE schemes have their ciphertexts grow linearly with the size of the embedded set of attributes. The exceptional one, unfortunately, only supports access policies of thresholds. In 2011, Attrapadung et al. [ALdP11] proposed the first KP-ABE scheme supporting non-monotonic access structures that has constant-sized ciphertexts. A trade-off for the succinct ciphertxts is that the size of private keys is quadratic to the number of attributes involved in their access policies.

For applications such audit log sharing, KP-ABE scheme provides a powerful tool for encryption with fine-grained access control, which also supports delegation of secret keys. Unfortunately, with a drawback that the access policy is built into the secret key, it is inconvenient for encryptors in a KP-ABE scheme to decide who can decrypt a ciphertext. In a certain degree, the control of the access of ciphertexts however depends more on the PKG.

3.1.2 Ciphertext-Policy Attribute-Based Encryption

The concept of CP-ABE was brought up by Goyal et al. [GPSW06] in 2006. In a CP-ABE scheme, a data owner encrypts messages and enforces access policies over attributes. A user is able to decrypt a ciphertext if his/her private key is associated with attributes that satisfy the access policy. Bethencourt et al. [BSW07] proposed the first CP-ABE scheme in 2007. Their construction can support access policies constructed from a monotonic access tree. Although their work achieved fine-grained access control, the security proof is provided in generic group model.

In the same year, Cheung and Newport [CN07] proposed the frist CP-ABE scheme that is proven secure under the standard model. Their work supports access policies of AND-gate and each attribute can be assigned to two values, as positive and negative to indicate if a user owns an attribute, while access policies are always involved with all attributes requesting if a potential decryptor should own or not own an attribute or an extra "do not care" value to indicate the attribute which does not appear in the AND-gate. Intuitively, the public parameters include three sets of components as T_i, T_{n+i}, and T_{2n+i} corresponding to the three types of occurrences of each attribute. This scheme is proven secure in IND-CPA secure model under the DBDH assumption. Compared with Bethencourt et al's work, the scheme has advantage in security proof but is less efficient and expressive as that the size of ciphertexts and private keys grows linearly with the total number of attributes and the access policy is restricted in logical conjuction.

Subsequently, Nishide et al. [NYO09] and Emura et al. [EMN+09] proposed different schemes based on Cheung and Newport's work. Nishide et al. improved the efficiency and equipped their work with a new feature of hidden access policy.

Emura et al.'s work offers constant-sized ciphertexts and constant-numbered bilinear pairing operations supporting access policies of AND-gate on multi-value attributes.

In 2008, Goyal et al. [GJPS08] adpoted bounded tree structure for access policies in CP-ABE to construct a more expressive scheme that can be proven secure under standard assumption. They defined a new notion as "Bounded CP-ABE" in their work and generalised a transformational approach that can trans form any KP-ABE schemes into CP-ABE using a special structure as they called "universal access tree". The access policies in the BCP-ABE scheme can cover all formulas of polynomial-bounded size, while the depth of the corresponding access tree needs to be bounded to a fixed number that is defined in Setup phase. In 2009, Liang et al. [LCLX09] improved the encryption and decryption algorithms of Goyal et al.'s BCP-ABE scheme and proposed a BCP-ABE scheme with shortened public parameters, private keys and ciphertexts.

To remove the boundary restricions in [GJPS08, LCLX09], Ibraimi et al. [ITHJ09] presented a new technique that realises the CP-ABE scheme without Shamir's threshold secret sharing. With their new technique, the access policy can then be defined by an n-ary tree access tree that is represented by "and" and "or" nodes. In their scheme, the decryption process is friendly to devices with restrained devices since polynomial interpolations from Shamir's secret sharing is a computationally-consuming calculation. There is an improvement in overall computation efficiency of their work compared with Cheung and Newport's [CN07].

In 2011, a new methodology was proposed by Waters [Wat11] to realise CP-ABE that is provenly secure under concrete and non-interactive assumption. In their scheme, the access policy is constructed by a linear secret sharing scheme over the descriptive attributes, which includes all previously used access policy structures. In this efficient scheme, the size of ciphertexts and private keys and the computation overhead of encryption and decryption process increase linearly with involved attributes, which makes his scheme achieve the same performance and functionality as Bethencourt et al.'s work [BSW07].

Lewko et al. [LOS$^+$10] then advanced Waters' work [Wat11] in encoding technique and proposed an ABE scheme that achieved adaptive security. In their scheme, the bilinear pairing system is based on composite order groups, which results in loss of practical usage.

Many of the schemes proposed in recent years are constructed based on bilinear pairings. A CP-ABE scheme that supports AND-gate without bilinear pairing system was proposed by Zhang and Zhang [ZZ11]. n-ary lattices is adopted to construct their scheme and offered a strong security proof based on worst-case hardness. Despite the efficiency of their work, it showed an alternative way of building ABE schemes from lattices, from which many new schemes were then proposed.

3.1.2.1 Comparison in Basic Attribute-Based Encryption Schemes

From what has been mentioned above, KP-ABE and CP-ABE schemes are different in complexity hypothesis, strategic flexibility, and applications. A comparison can be made as follows.

The first ABE scheme supports only threshold policy and suits when applications require simple policies. KP-ABE and CP-ABE schemes support complex access policies and suit when applications require fine-grained access control. In addition, access policies are embedded into private keys in KP-ABE, so a data owner cannot assign the access control to ciphertexts. Compared with KP-ABE schemes, CP-ABE schemes are more suitable for the realistic scenes in favor of data owners. KP-ABE schemes apply to query applications, such as pay TV system, audit log, targeted broadcast, and database access. On the contrary, CP-ABE schemes are used for access control applications, such as social networking site access, and electronic medical system.

The first ABE scheme and early KP-ABE schemes [GPSW06, OSW07] are based on the DBDH assumption, while the situation in CP-ABE schemes is more complex. The construction of CP-ABE will be more complex and its security will be more difficult to prove if the supported type of access policies goes more complicated. To achieve the CPA security under the standard complexity assumption, the main research on the CP-ABE is focused on designing the access structure. According to different access structures, the research can be divided into three kinds: AND-gate, access tree, and LSSS matrix. Now a comparison of Access structure, Complexity assumption, Security model, and Supported policy in different CP-ABE schemes is made in Table 3.1.

Table 3.1: Comparison of expression complexity and security assumptions in different CP-ABE schemes

Scheme	Access structure	Assumption	Model	Boolean Op.
[CN07]	AND gate	DBDH	Selective	And, Not
[NYO09]	AND gate	DBDH, D-linear	Selective	And
[EMN+09]	AND gate	DBDH	Selective	And
[BSW07]	Unbounded Tree	Generic group	Adaptive	And, Or, Threshold
[ITHJ09]	Unbounded Tree	DBDH	Selective	And, Or, Threshold
[GJPS08]	Bounded Tree	DBDH	Selective	And, Or, Threshold
[LCLX09]	Bounded Tree	DBDH	Selective	And, Or, Threshold
[Wat11]	LSSS matrix	DPBDHE	Selective	And, Or, Threshold
[LOS+10]	LSSS matrix	3P-SDP	Adaptive	And, Or, Threshold

The comparison of the size of public parameters and master secret keys in different CP-ABE schemes is given in Table 3.2. The comparison of the size of private keys and ciphertexts in different CP-ABE schemes is shown in Table 3.3. The com-

parison of the computational overheads of the encryption and decryption process in different CP-ABE schemes is made in Tables 3.4. We can draw a conclusion from these tables: Emura et al.'s [EMN+09] scheme is the shortest in ciphertexts and private keys, Bethencourt et al.'s [BSW07] in params, and Waters' [Wat11] in msk. In addition, in Bethencourt et al.'s [BSW07], params and msk have nothing to do with system attributes. As for computation overhead, Emura et al.'s [EMN+09] processes the lowest encryption/decryption overhead, and Ibraimi et al.'s [ITHJ09] scheme has a lower one than Waters' [Wat11].

Table 3.2: Comparison of size of public parameters and master secret keys in different CP-ABE schemes

Scheme	params	msk
[CN07]	$(3n+1)L_{\mathbb{G}_1} + L_{\mathbb{G}_2}$	$(3n+1)L_{\mathbb{Z}_p}$
[NYO09]	$(2nm+1)L_{\mathbb{G}_1} + L_{\mathbb{G}_2}$	$(2nm+1)L_{\mathbb{Z}_p}$
[EMN+09]	$(nm+2)L_{\mathbb{G}_1} + L_{\mathbb{G}_2}$	$(nm+1)L_{\mathbb{Z}_p}$
[BSW07]	$3L_{\mathbb{G}_1} + L_{\mathbb{G}_2}$	$L_{\mathbb{Z}_p} + L_{\mathbb{G}_1}$
[ITHJ09]	$(n+1)L_{\mathbb{G}_1} + L_{\mathbb{G}_2}$	$(n+1)L_{\mathbb{Z}_p}$
[Wat11]	$(n+2)L_{\mathbb{G}_1} + L_{\mathbb{G}_2}$	$L_{\mathbb{G}_1}$
[LOS+10]	$(n+2)L_{\mathbb{G}_1} + L_{\mathbb{G}_2}$	$L_{\mathbb{Z}_p} + L_{\mathbb{G}_1}$

n : Total number of attributes in systems;
m: Total number of possible values of an attribute in systems;
A_C: The set of attributes involved in the access policy of a ciphertext;
A_U: The set of attributes included in a user's private key;
L_*: Bit length of element in *.

Table 3.3: Comparison of size of private keys and ciphertexts in different CP-ABE schemes

Scheme	sk	CT
[CN07]	$(2n+1)L_{\mathbb{G}_1}$	$(n+1)L_{\mathbb{G}_1} + L_{\mathbb{G}_T}$
[NYO09]	$(3n+1)L_{\mathbb{G}_1}$	$(2nm+1)L_{\mathbb{G}_1} + L_{\mathbb{G}_T}$
[EMN+09]	$2L_{\mathbb{G}_1}$	$2L_{\mathbb{G}_1} + L_{\mathbb{G}_T}$
[BSW07]	$(2\|A_U\|+1)L_{\mathbb{G}_1}$	$(2\|A_C\|+1)L_{\mathbb{G}_1} + L_{\mathbb{G}_T}$
[ITHJ09]	$(\|A_U\|+1)L_{\mathbb{G}_1}$	$(\|A_C\|+1)L_{\mathbb{G}_1} + L_{\mathbb{G}_T}$
[Wat11]	$(\|A_U\|+2)L_{\mathbb{G}_1}$	$(2\|A_C\|+1)L_{\mathbb{G}_1} + L_{\mathbb{G}_T}$
[LOS+10]	$(\|A_U\|+2)L_{\mathbb{G}_1}$	$(2\|A_C\|+1)L_{\mathbb{G}_1} + L_{\mathbb{G}_T}$

n : Total number of attributes in systems;
m: Total number of possible values of an attribute in systems;
A_C: The set of attributes involved in the access policy of a ciphertext;
A_U: The set of attributes included in a user's private key;
L_*: Bit length of element in *.

Table 3.4: Comparison of performance in different CP-ABE schemes

Scheme	Encryption	Decryption
[CN07]	$(n+1)\mathbb{G}_1 + 2\mathbb{G}_T$	$(n+1)C_e + (n+1)\mathbb{G}_T$
[NYO09]	$(2nm+1)\mathbb{G}_1 + 2\mathbb{G}_T$	$(3n+1)C_e + (3n+1)\mathbb{G}_T$
[EMN$^+$09]	$(n+1)\mathbb{G}_1 + 2\mathbb{G}_T$	$2C_e + 2\mathbb{G}_T$
[BSW07]	$(2\|A_C\|+1)\mathbb{G}_1 + 2\mathbb{G}_T$	$2\|A_U\|C_e + (2\|S\|+2)\mathbb{G}_T$
[ITHJ09]	$(\|A_C\|+1)\mathbb{G}_1 + 2\mathbb{G}_T$	$(\|\omega\|+1)C_e + (\|\omega\|+1)\mathbb{G}_T$
[Wat11]	$(4\|A_C\|+1)\mathbb{G}_1 + 2\mathbb{G}_T$	$2\|A_U\|C_e + 3\|A_U\|\mathbb{G}_T$
[LOS$^+$10]	$(4\|A_C\|+1)\mathbb{G}_1 + 2\mathbb{G}_T$	$2\|A_U\|C_e + 3\|A_U\|\mathbb{G}_T$

n: Total number of attributes in systems;
m: Total number of possible values of an attribute in systems;
A_C: The set of attributes involved in the access policy of a ciphertext;
A_U: The set of attributes included in a user's private key;
C_e: bilinear paring operation;
S: Least interior nodes satisfying an access structure;
ω: Least subset of attributes satisfying an access structure;

3.2 Previous ABE Schemes Supporting Supplemental Functionalities

In this section, we survey existing significant ABE schemes supporting supplemental functionalities related to this thesis, namely accountability and revocation mechanism.

3.2.1 Accountability

At present, accountable ABE schemes can be divided into two kinds: accountable CP-ABE schemes [LRK09, LRZW09, LHC$^+$11] and accountable KP-ABE schemes [YRLL09, WCLL12].

3.2.1.1 Accountable Ciphertext-Policy Attribute-Based Encryption

Li et al. [LRZW09] first proposed the notion of accountable CP-ABE to address the problem of key abuse in ABE system. In their ciphertext-policy accountable attribute-based encryption (CP-A^{2}BE) scheme, personal information or user-specific information is embedded in private keys to ensure user accountability. This user-related information can be simply a user identity. When a user shares his private key, his/her identity will then be detected from a pirated device if the shared key is maliciously used. The tracing algorithm in their work presumes a specific format

to the key used to trace, which leads to a white-box tracking functionality. In addition, it has a limited ability to express access policies and it needs public key certificate authority for issuing certificates for all users, which has a serious impact on performance.

Later, Li et al. [LRZW09] improved their tracing mechanism for illegal key sharing among users and proposed the notion of ciphertext-policy accountable and anonymous attribute-based encryption (CP-A^{3}BE). The concept behind CP-A^{3}BE is similar compared with CP-A^{2}BE that a user private key will include a user identity. In the proposed CP-A^{3}BE scheme, tracing functionality was improved to black-box model and the anonymous feature is also included. The only disadvantage is that the length of the private keys and ciphertexts are increased.

In 2011, Li et al. [LHC$^+$11] further enhanced their previous work so that the proposed scheme can support multiple authorities while remain the feature of user accountability. In their scheme, one can trace the identity of a misbehaving user who leaks his/her private key and the trust assumptions on both authorities and users can be reduced. The tracing process is efficient as it has a lower computational overheads compared with the existing accountable ABE schemes.

3.2.1.2 Accountable Key-Policy Attribute-Based Encryption

Key abuse attacks also impede the wide applications of KP-ABE especially in copyright-sensitive systems.

Yu et al. [YRLL09] proposed the notion of abuse free key-policy attribute-based encryption (AFKP-ABE) to defend key abuse attacks in KP-ABE. In their scheme, hidden attributes are introduced to identify single user piracy or partial colluding users. Their tracing algorithm does not require any specific format of private keys and enables black-box tracking functionality. Its performance is efficient if the number of total users is not too large since the size of its secret keys and ciphertexts is the logarithm of the total number of users. Their scheme is proven secure under the DBDH assumption and the D-linear assumption.

Recently, Wang et al. [WCLL12] first presented an accountable authority KP-ABE scheme which is proved secure under the modified Bilinear Decisional Diffie-Hellman assumption in the standard model.

3.2.1.3 Comparison

Regarding trace mode, trace target, security assumption and types of access structure, a comparison of the CP-A^{2}BE [LRK09], CPA^{3}BE [LRZW09], and AFKP-ABE [YRLL09] is given in Table 3.5, from which we can draw conclusions below. First, all of these three schemes can achieve user accountability. Second, as a result of early

Table 3.5: Comparison of CP-A^{2}BE, CP-A^{3}BE and AFKP-ABE

Scheme	Trace mode	Trace target	Assumption	Access structure
[LRK09]	White box	Authority, user	DBDH, CDH	And
[LRZW09]	Black box	user	DBDH, D-linear	And
[YRLL09]	Black box	user	DBDH, D-linear	And, or, threshold

work, the CP-A^{2}BE scheme requires a format specification of private keys in tracing algorithm, which makes it less feasible in practice. Finally, both the CP-A^{3}BE and the AFKP-ABE protect the sender's privacy, but the later can only partially hide attributes.

3.2.2 Revocation Mechanism

In multi-user encryption systems, a revocation mechanism is a useful tool to manage malicious behaviours. In ABE system, it is more difficult to realise the revocation mechanism since it is more complicated than constructing it in traditional public key cryptosystem or IBE schemes [BGK08, Mic96, ALO98, NNL01, LV09]. For example, in CP-ABE schemes, different users may hold private keys with the same attributes, leading to additional difficulties in design of a revocation mechanism.

In attribute-based setting, revocation mechanism can usually be divided into two kinds: user revocation and attribute revocation. Currently, there are mainly two ways to realise them [AI09a]: one is the indirect revocation method [BSW07, PTMW10, BGK08, IPN$^+$09, YWRL10, HN11, XMLC13] and the other is the direct revocation method [OSW07, AI09b, LLLS10, QM12].

3.2.2.1 Indirect Revocation Method

A revocation mechanism from the indirect revocation method requires the authority to release information for key update periodically to non-revoked users, while implicitly revoking users as they cannot update their private keys. The advantage of the indirect method is that the senders do not need to know the revocation list. The disadvantage is that the key update needs to set up communications from the authority to all non-revoked users periodically, which may result in a bottle neck if the update cycle is too short or there are too many users in the system. Many attribute revocable ABE schemes have been proposed based on the indirect revocation method [BSW07, PTMW10, BGK08, IPN$^+$09, YWRL10, HN11, XMLC13].

Early works [BSW07, PTMW10, BGK08] adopted the concept of expiration time on each attribute to realise attribute revocation. These schemes have two main problems. One is the security degradation in terms of the backward and forward security [HN11]. The other is the scalability problem. To reduce the burden of

authority, two CP-ABE schemes with immediate attribute revocation with the help of semi-honest service provider were proposed by Ibraimi et al. [IPN+09] and Yu et al. [YWRL10]. But their works can only support simple access policies while the data outsoucing environment requires fine-grained access control.

Later, Hur and Noh [HN11] proposed a CP-ABE scheme with fine-grained access control and attribute revocation with the help of the honest-but-curious proxy deployed in the data service provider. In their scheme, the method of using the structure of binary tree for efficient revocation [BGK08] is adopted for an efficient revocation mechanism. Unfortunately, their scheme cannot resist the collusion attack.

In 2013, Xie et al. [XMLC13] proposed a new CP-ABE scheme that supports efficient user and attribute revocation. They improved the computation overhead in the key update phase, which is halved comapred with Hur and Noh's work [HN11].

3.2.2.2 Direct Revocation Method

A revocation mechanism from the direct revocation method requires a sender to specifies the revocation list when a ciphertext is being encrypted. The advantage of the direct method is that it does not require all non-revoked users to update their keys periodically as what happens when the indirect method is adopted. The disadvantage is that it needs the sender to keep and manage the current revocation list, which could be a troublesome task. Many attribute revocable ABE schemes [OSW07, AI09b, LLLS10, QM12] that used the direct mode have been proposed.

In KP-ABE, senders are only allowed to specify a set of attributes to ciphertexts which makes it not possible yet to construct a direct revocation mechanism. Staddon et al. [SGGR08] suggested a KP-ABE scheme with direct revocation mechanism. Their work is restricted to a condition that the number of attributes assigned to the set of attributes of a ciphertext is equal to half of the size of the attribute universe.

In CP-ABE, a trivial construction of direct revocation mechanism can be built by using Ostrovsky et al.'s [OSW07]. Since Ostrovsky et al.'s [OSW07] supports negative clauses, negation of revoked user identities or attributes can then be added conjunctively to the AND-gate. This trivial solution is low in efficiency since the length of the ciphertexts scales with the increased revoked users or attributes.

Attrapadung and Imai [AI09b] suggested a different concept of combining broadcast encryption with ABE scheme to achieve user revocation. In their proposed scheme, all the membership lists for each attribute group is maintained by the data owner to enable the direct user revocation. Subsequently, Liang et al. [LLLS10] proposed a CP-ABE scheme with efficient revocation mechanism. In their scheme, linear secret sharing and binary tree techniques are combined and each user is assigned a unique identifier for efficient revocation.

The three typical CP-ABE schemes with direct revocation [OSW07, AI09b, LLLS10] all support user revocation, and they have no effect on attribute revocation. In 2012, Wu and Zhang [QM12] first formalised the notion of attribute-based encryption supporting attribute revocation under direct revocation mode.

Chapter 4

Efficient and Expressive Ciphertext-Policy Attribute-Based Encryption Supporting Threshold and AND-gate

Most of the existing expressive CP-ABE schemes produce long ciphertexts, which affects their efficiency and applications. In this chapter, this gap of efficiency and expressiveness is considered and a CP-ABE scheme that outputs constant-size ciphertext and supports access policies of an AND-gate and a threshold is proposed. The proposed scheme is efficient, expressive and secure. In our construction, the supported access policy include two sets of attributes S_1 and S_2 over an attribute universe and a threshold value t_1. The access policy is satisfied if a user owns at least t_1 attributes in S_1 and all the attributes in S_2. The scheme is IND-sCPA secure proved in the standard model under the augmented multi-sequence of exponents decisional Diffie-Hellman assumption.

4.1 Background and Scenario

In the era of big data, CP-ABE becomes a promising technology enabler to meet the need for sharing and storing sensitive data on the Internet ubiquitously. Although the functionality provided by CP-ABE fits many real world scenarios, the applications of CP-ABE have been limited due to efficiency drawbacks shared by most CP-ABE schemes that the size of ciphertexts increases linearly with the number of involved attributes. This limitation can be seen in a simple comparison of needed storage space in one-to-many encryption between traditional encryption and attribute-based encryption. If traditional encryption is adopted, a message will be encrypted many times according to the number of recipients, of which the storage space is then increased linearly in the number of recipients. Compared with attribute-based encryption, if the number of recipients is not large while a large number of attributes are used to describe access policies, the significance of attribute-based encryption becomes less attractive.

So far, researchers have tried to construct different schemes for constant-sized CP-ABE, but the access policies supported by theses schemes can either be a single AND-gate or a single threshold. If a scheme can only support access policies of a single threshold, all attributes become *optional* and decryption process will suc-

ceed when many enough attributes are included in the used private key while no specific attribute can be enforced along with the threshold. If a scheme can only support access policies of a single AND-gate, all attributes become *mandatory* and decryption process requires all of the attributes included in an access policy to be also included in the decryption private key. Currently, there is no CP-ABE scheme with short ciphertexts addressing further expressive access policies. However, in a concrete application, access policies may need to be defined with both mandatory and optional attributes, and hence, a threshold and AND-gate policy.

To illustrate this situation, consider the following outsourcing scenario[a]. A client would like to develop a project, and hence, this client will register to an outsourcing project platform. In this platform, there are many freelancers, who are offering their service. Each freelancer will gain his/her attribute during the registration process, and the attribute is something like "IT/software", "senior programmer", "C/C++", "Java". When the client outsources his/her job to the outsourcing platform, the client needs to specify the requirements of the freelancer that will do the task. As an example, the client requires the task to be conducted by a senior freelancer in IT/software group with at least three expertises of "C/C++ Programming", "JAVA", "Mobile App" and "Software Development". This means, the corresponding access policy can then be defined by a set of mandatory attributes {IT group, Senior}, a set of optional attributes {C/C++ Programming, JAVA, Mobile App, Software Development} and a threshold value 3 as showed in Fig. 4.1. The client should be able to use a CP-ABE scheme with the above access policy to encrypt the task, and subsequently, the freelancers who satisfy the access policy should be able to read this message and then do the task.

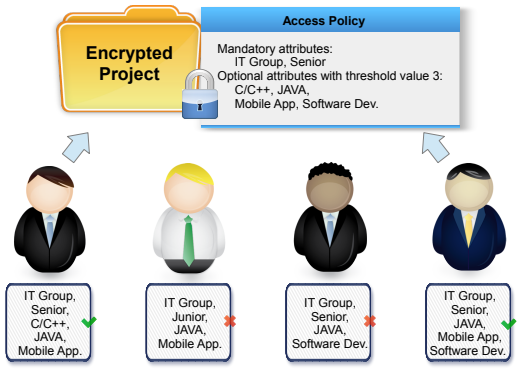

Figure 4.1: An example of users getting access to an encrypted project according to its access policy.

The first set of attributes describes an AND-gate policy, and the second set of attributes with the threshold value describes a threshold policy, which need to be

[a]This example is illustrated based on the rent-a-coder website: http://www.rent-acoder.com/.

satisfied if a user wants the details of the project. If the adopted CP-ABE scheme can only support threshold policy, then no mandatory attributes can be put into access policies, like the attribute "IT group" and "Senior" in the above example. On the other hand, if the CP-ABE scheme can only support an AND-gate policy, the project will then be encrypted repeatedly for all accepted combinations of expertise with the mandatory attributes. We note that producing constant-size ciphertexts will be an important and desired property for enabling such a scheme that supports both mandatory and optional attributes, or else the scheme will be much less practical as the size of the encrypted metadata (e.g a symmetric key) should be retained.

Trivial Constructions. Since several works have already achieved short ciphertexts CP-ABE schemes supporting a single AND-gate or a single threshold access policies, one may think that obtaining a short ciphertext CP-ABE scheme supporting a threshold and AND-gate policy can be done by a simple combination of the two schemes. However, the resulting scheme from this approach could be easily attacked as it is possible to launch a collusion attack with one key satisfying the AND-gate and another key satisfying the threshold, while actually they do not satisfy the required *combined* access policy.

Our Techniques. When constructing a CP-ABE scheme supporting a threshold and AND-gate access policy with short ciphertexts, the following technical hurdles must be overcome.

First, the scheme must produce constant-size ciphertexts despite the number of involved attributes. We exploit the "aggregate" technique from [DP08] and the "dummy attribute" technique from [HLR10] to form the upper bound of the size of ciphertexts. To encrypt with a threshold and AND-gate access policy, we construct two group elements in ciphertexts. One is associated with all optional attributes in the threshold S_1 as well as $n-1-|S_1|+t_1$ dummy attributes, where n is the maximal number of attributes and t_1 is the threshold value. The other one is associated with all mandatory attributes in the AND-gate attribute set S_2. In decryption, private key components are aggregated into two group elements as well for computation.

Second, the collusion attacks must not exist. In our construction, an old-fashioned technique is adopted that each private key has its sets of components bound to each other with some random numbers that sum up to a unique fixed number, which makes components from different keys incompatible. In addition, we construct different sets of key components based on different generators in each private key to prevent collusion attacks within a private key itself.

4.1.1 Related Work

Most of the previous ABE systems produce long ciphertexts, which grow with the number of attributes involved in encryption process. In recent years, ABE schemes with constant-size ciphertexts have received much attention for applications in practical scenarios [ALdP11, CCL+13, LXZZ13, RD13a, AL10, CZF11, EMN+09, GZC+12, HLR10, RD13b, TDM12].

Emura et al. [EMN+09]proposed the first ABE scheme with constant-size ciphertexts, which is a CP-ABE scheme supporting an AND-gate policy of multiple-value attributes. In their scheme [EMN+09], a disadvantage is that a user can decrypt only if his/her private key is associated with a set of attributes that is identical to the access policy of the ciphertext. Therefore, their scheme can be seen as an ABE scheme with private keys and ciphertexts both constrained with an AND-gate policy, which reduces the flexibility significantly. Similarly, the CP-ABE schemes [TDM12] also share the same disadvantage as the scheme [EMN+09]. To prevail over this disadvantage, Chen et al. [CZF11] proposed a CP-ABE scheme supporting AND-gate policies that enjoys constant computation cost and constant-size ciphertexts.

Herranz et al. [HLR10] proposed a dynamic (l, n)-threshold CP-ABE scheme that produces constant-size ciphertexts. In their scheme, an algorithm Aggregate from [DP08] is adopted for decryption which requires $\mathcal{O}(l^2)$ exponentiation computation. Ge et al. [GZC+12] proposed a new (l, n)-threshold CPA-secure CP-ABE scheme with constant-size ciphertexts. Although their construction can be extended to a CCA-secure scheme, the size of private keys in their schemes has quadratic growth based on the number of attributes associated. For more expressive or general decryption policies, no existing CP-ABE scheme has short ciphertexts. This fact can limit the applications of ABE in real life, if only a low bandwidth is available.

Chapter Organisation. This chapter is organised as follows: In Section 4.2, we provides background definitions related to CP-ABE system. In Section 4.3 the adopted computational assumption is described, on which the security of our scheme will be based. In Section 4.4 our CP-ABE construction is presented, where we also proved its security in standard model. Section 4.5 discusses the efficiency and performance of the proposed scheme. Section 4.6 contains the proof of the intractability of the adopted aMSE-DDH problem. The chapter is concluded in Section 4.7.

4.2 The Augmented Multi-sequence of Exponents Diffie-Hellman Assumption

The security of our scheme is reduced to the hardness of a problem, which we called the augmented multi-sequence of exponents decisional Diffie-Hellman problem. The

problem is modified from the (l, m, t)-aMSE-DDH problem defined in [HLR10], of which the generic complexity is covered by the general Diffie-Hellman exponent theorem due to Boneh et al. [BBG05], as the problem lies in the scope of their framework.

Let $\mathbb{S} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(\cdot,\cdot))$ be a bilinear map group system. Let g_0 be a generator of $\mathbb{G}_1$ and h_0 be a generator of $\mathbb{G}_2$. Let n, s_1, s_2, t_1 be four integers where $n >= s_1 + s_2$ and $s_1 >= t_1$. The (n, s_1, s_2, t_1)-*augmented multi-sequence of exponents decisional Diffie-Hellman* ((n, s_1, s_2, t_1)-aMSE-DDH) *problem* related to $\mathbb{S}$ is as follows:

Input The vector $\overrightarrow{x}_{2n-1-s_1+t_1} = (x_1, \ldots, x_{2n-1-s_1+t_1})$ defines the co-prime polynomials, of which the components are pairwise distinct elements of $\mathbb{Z}_p$,

$$f(X) = \prod_{i=1}^{n-s_1-s_2} (X + x_i), \qquad g_1(X) = \prod_{i=n-s_1-s_2+1}^{n-s_2} (X + x_i),$$
$$g_2(X) = \prod_{i=n-s_2+1}^{n} (X + x_i), \qquad h_1(X) = \prod_{i=n+1}^{2n-1-s_1+t_1} (X + x_i),$$

the values

$$\begin{cases}
g_0, g_0^{\gamma}, \ldots, g_0^{\gamma^{2n-s_1+t_1-3}}, \quad g_0^{\kappa\cdot\gamma\cdot f(\gamma) g_2(\gamma)}, & (4.1.1)\\
g_0^{\alpha\cdot g_2(\gamma)\cdot\gamma^0}, \ldots, g_0^{\alpha\cdot g_2(\gamma)\cdot\gamma^{n-s_1-s_2+1}}, & (4.1.2)\\
g_0^{\omega\cdot\gamma}, \ldots, g_0^{\omega\cdot\gamma^n}, & (4.1.3)\\
g_0^{\frac{\kappa\gamma f(\gamma) g_1(\gamma)}{\zeta}}, & (4.1.4)\\
g_0^{\frac{g_1(\gamma)\cdot\alpha\gamma^0}{\zeta}}, \ldots, g_0^{\frac{g_1(\gamma)\cdot\alpha\cdot\gamma^{n-s_1-s_2+1}}{\zeta}}, & (4.1.5)\\
g_0^{\frac{\omega\gamma^0}{\zeta}}, \ldots, g_0^{\frac{\omega\gamma^{n-1}}{\zeta}}, & (4.1.6)\\
h_0^{g_1(\gamma)\cdot\gamma^0}, \ldots, h_0^{g_1(\gamma)\cdot\gamma^{n+t_1-3}}, \quad h_0^{\kappa\cdot g_1^2(\gamma) h_1(\gamma)}, & (4.1.7)\\
h_0^{\alpha\cdot g_1(\gamma)\cdot\gamma^0}, \ldots, h_0^{\alpha\cdot g_1(\gamma)\cdot\gamma^{2n-1}}, & (4.1.8)\\
h_0^{\omega\cdot g_1(\gamma)\cdot\gamma^0}, \ldots, h_0^{g_1(\gamma)\cdot\omega\cdot\gamma^{n+s_1-1}}, & (4.1.9)\\
h_0^{\zeta\cdot h_1(\gamma)\cdot g_1(\gamma)\cdot\gamma^0}, \ldots, h_0^{\zeta\cdot h_1(\gamma)\cdot g_1(\gamma)\cdot\gamma^{s_2-2}}, & (4.1.10)\\
h_0^{\zeta\cdot\alpha\cdot g_2(\gamma)\cdot\gamma^0}, \ldots, h_0^{\zeta\cdot\alpha\cdot g_2(\gamma)\cdot\gamma^{2n-1}}, & (4.1.11)\\
h_0^{g_1(\gamma)\cdot\frac{\zeta\cdot h_1(\gamma)-1}{\gamma}}, \quad h_0^{\zeta\kappa g_2^2(\gamma)} & (4.1.12)
\end{cases}$$

where κ, ζ, ω, α, γ are unknown random elements of $\mathbb{Z}_p$, element $T_b = e(g_0, h_0)^{\kappa\cdot f(\gamma) g_1(\gamma) g_2(\gamma)} \in \mathbb{G}_T$ and a random group element $T_{1-b} \in \mathbb{G}_T$ while b is a fair coin.

Output a bit b'. The problem is correctly solved if the output is $b' = b$.

The following statement is a corollary of Theorem 2.30. It provides an intractability bound in the generic model, but in groups equipped with pairings. A

full proof of its intractability is given in Section 4.6.1. We emphasize on the fact that, whereas the assumption has several parameters, it is non-interactive, and thus easily falsifiable [Nao03].

Corollary 4.1 (Generic Security)**.** *For any probabilistic algorithm $\mathcal{B}$ that makes at most q_G queries to the oracles performing group operations in $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ and the bilinear map $e(\cdot,\cdot)$, its advantage in solving $(n,\ s_1,\ s_2,\ t_1)$-aMSE-DDH problem is bounded as*

$$\mathsf{Adv}_{\mathcal{B}}^{\mathsf{aMSE\text{-}DDH}}(\lambda) \leq \frac{(q_G + 12n - 2s_1 - s_2 + 2t_1 + 7)^2 \cdot d}{2p}$$

where $d = \max(2(2n + s_1 + 1), 2(2n + s_2 + 2))$.

4.3 Construction

In this section, we shall present our ciphertext-policy attribute-based encryption scheme.

4.3.1 Introduction to the aggregation algorithm

Before presenting the details of our construction, we introduce the adopted algorithm Aggregate of [DP08] for the decryption process. This algorithm is given for group elements in $\mathbb{G}_T$ [DP08], but it can be seen that it works in any group of prime order.

$\mathsf{Aggregate}(\{g^{\frac{r}{\gamma+x_i}}, x_i\}_{1\leq i\leq l})$ The algorithm takes as input a list of values $\{g^{\frac{r}{\gamma+x_i}}, x_i\}_{1\leq i\leq l}$, where $g^{\frac{r}{\gamma+x_i}} \in \mathbb{G}_1$, x_i are pairwise distinct and $r, \gamma \in \mathbb{Z}_p$ are unknown. It outputs the value

$$\mathsf{Aggregate}(\{g^{\frac{r}{\gamma+x_i}}, x_i\}_{1\leq i\leq l}) = g^{\frac{r}{\prod_{i=1}^{l}(\gamma+x_i)}} \in \mathbb{G}_1.$$

Here we give the details of the algorithm Aggregate. Given x_i and $g^{\frac{r}{\gamma+x_i}}$ for $i = 1, \ldots, l$, let us define for any (j,k) such that $1 \leq j < k \leq l$

$$B_{j,k} = \left(g^{\frac{r}{\gamma+x_k}}\right)^{\frac{1}{\prod_{i=1}^{j}(\gamma+x_i)}} = \left(\frac{B_{j-1,j}}{B_{j-1,k}}\right)^{\frac{1}{x_k - x_j}}.$$

The algorithm poses $B_{0,k} = g^{\frac{r}{\gamma+x_k}}$ for $k = 1, \ldots, l$ and computes sequentially $B_{j,k}$ for $j = 1, \ldots, l-1$ and $k = j+1, \ldots, l$ using the above induction. The algorithm finally outputs $g^{\frac{r}{\prod_{i=1}^{l}(\gamma+x_i)}} = B_{l-1,l}$. Note that a successful run of the Aggregate algorithm requires $x_j \neq x_k$ for $1 \leq j < k \leq l$. If there exists $x_j = x_k$ for some $j < k$ then $B_{j-1,j} = B_{j-1,k}$, and $B_{j,k}$ contains a factor of $(\gamma + x_j)^2$ in the denominator of

its exponent which makes it infeasible to compute without knowing γ. It can be seen that the algorithm requires l^2 operations of group exponentiation to carry out the result.

4.3.2 Description

$\mathsf{Setup}(1^\lambda, \mathcal{P})$ The PKG chooses a suitable encoding τ sending each attribute in $\mathcal{P}$ onto a (different) element $\tau(A_i) = \delta \in \mathbb{Z}_p$. It also chooses a bilinear group system $\mathbb{S} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(\cdot,\cdot))$. It picks at random $\eta \in \mathbb{Z}_p$ and two generators g of $\mathbb{G}_1$ and h of $\mathbb{G}_2$, and set $g' = g^{\frac{1}{\eta}}$ and $h' = h^\eta$.

After that, a set $\mathcal{D} = \{d_1, \ldots, d_{n-1}\}$ is chosen consisting of $n-1$ pairwise different elements of $\mathbb{Z}_p$, which must also be different to the values $\tau(A_i)$, for all attributes in $\mathcal{P}$. For any integer i lower or equal to $n-1$, we denote as $\mathcal{D}_i$ the set $\{d_1, ..., d_i\}$.

Next, the PKG picks at random $\alpha, \gamma \in \mathbb{Z}_p$ and sets $u = g^{\alpha\gamma}$, $u' = g'^{\alpha\gamma}$ and $Y = e(g^\alpha, h)$. The master secret key is then $\mathsf{msk} = (g, \alpha, \gamma, \eta)$ and the public parameters are

$$\mathsf{params} = \left(\mathcal{P}, n = |\mathcal{P}|, u, Y, \{h^{\alpha\gamma^i}, h'^{\alpha\gamma^i}\}_{i=0,\ldots,2n-1}, \mathcal{D}, \tau\}\right).$$

$\mathsf{KeyGen}(\mathsf{params}, W, \mathsf{msk})$ Given any subset $W \subset \mathcal{P}$ of attributes, the PKG picks $r_1, r_2 \in \mathbb{Z}_p$ at random, computes $r_3 = 1 - r_2 \in \mathbb{Z}_p$ and outputs the private key sk_W of

$$\left(\{g^{\frac{r_1}{\gamma+\tau(A_i)}}, g'^{\frac{r_3}{\gamma+\tau(A_i)}}\}_{A_i \in W}, \{h^{r_1\gamma^i}\}_{i=0,\ldots,n-2}, h^{\frac{r_1-r_2}{\gamma}}\right).$$

$\mathsf{Enc}(\mathsf{params}, \mathbb{A}, M)$ Given a threshold and AND-gate access structure of two sets $S_1, S_2 \subset \mathcal{P}$ with $s_1 = |S_1|, s_2 = |S_2|$ and a threshold value t_1 satisfying $1 \leq t_1 \leq s_1$, and a message $M \in \mathbb{G}_T$, the sender picks at random $\kappa \in \mathbb{Z}_p$ and computes

$$\begin{cases} C_1 = u^{-\kappa}, \\ C_1' = u'^{-\kappa}, \\ C_2 = h^{\kappa\cdot\alpha\cdot\prod_{A\in S_1}(\gamma+\tau(A))\prod_{d\in\mathcal{D}_{n+t_1-1-s_1}}(\gamma+d)}, \\ C_3 = h'^{\kappa\cdot\alpha\cdot\prod_{A\in S_2}(\gamma+\tau(A))}, \\ C_m = M\cdot Y^\kappa \end{cases}$$

The value C_2 and C_3 are computed from the public parameters $(\{h^{\alpha\gamma^i}, h'^{\alpha\gamma^i}\}_{i=0,\ldots,2n-1})$. The ciphertext is then $CT = (\mathbb{A}, C_m, C_1, C_1', C_2, C_3)$.

$\mathsf{Dec}(\mathsf{params}, CT, sk_W)$ Any user with a set of attributes W such that $W \models \mathbb{A}$ can use the private key to decrypt the ciphertext.

To decrypt the ciphertext, the user need to compute $e(g,h)^{\kappa\cdot\alpha} = e(g,h)^{\kappa\cdot\alpha\cdot r_2} \cdot e(g',h')^{\kappa\cdot\alpha\cdot r_3}$.

First, the user computes $e(g,h)^{\kappa\cdot\alpha\cdot r_2}$ as follows. Let W_{S_1} be any subset of $W \cap S_1$ with $|W_{S_1}| = t_1$. The user computes

$$\mathsf{Aggregate}(\{g^{\frac{r_1}{\gamma+\tau(A_i)}}, \tau(A_i)\}_{A_i\in W_{S_1}}) = g^{\frac{r_1}{\prod_{A_i\in W_{S_1}}\gamma+\tau(A_i)}}.$$

With the aggregated output the user then computes

$$L_1 = e(g^{\frac{r_1}{\prod_{A_i\in W_{S_1}}\gamma+\tau(A_i)}}, C_2).$$

Next, a polynomial $P_{(W_{S_1},S_1)}(X)$ is defined in γ as

$$P_{(W_{S_1},S_1)}(\gamma) = \frac{1}{\gamma}\left(V_{(W_{S_1},S_1)}(\gamma) - v_{(W_{S_1},S_1)}\right).$$

where $V_{(W_{S_1},S_1)}(\gamma) = \prod_{A_i\in S_1\setminus W_{S_1}}(\gamma+\tau(A_i))\prod_{d\in\mathcal{D}_{n-1+t_1-s_1}}(\gamma+d)$ and $v_{(W_{S_1},S_1)} = \prod_{A_i\in S_1\setminus W_{S_1}}\tau(A_i)\prod_{d\in\mathcal{D}_{n-1+t_1-s_1}} d$.

Since $\deg V_{(W_{S_1},S_1)}(\gamma) = s_1 - t_1 + n - 1 + t_1 - s_1 - 1 = n-2$, the user can compute $h^{r_1 P_{(W_{S_1},S_1)}(\gamma)}$ from the values $\{h^{r_1\gamma^i}\}_{i=0,\ldots,n-2}$ in sk_W. After that, the user computes

$$L_2 = \left(e(C_1, h^{r_1 P_{(W_{S_1},S_1)}(\gamma)}) \cdot L_1\right)^{\frac{1}{v_{(W_{S_1},S_1)}}}$$
$$e(g,h)^{\kappa\cdot\alpha\cdot r_2} = e(C_1, h^{\frac{r_1-r_2}{\gamma}}) \cdot L_2$$

Second, the user computes $e(g',h')^{\kappa\cdot\alpha\cdot r_3}$. The user computes

$$\mathsf{Aggregate}(\{g'^{\frac{r_3}{\gamma+\tau(A_i)}}, \tau(A_i)\}_{A_i\in S_2}) = g'^{\frac{r_3}{\prod_{A_i\in S_2}\gamma+\tau(A_i)}}.$$

With the aggregated output the user then computes

$$e(g',h')^{\kappa\cdot\alpha\cdot r_3} = e(g'^{\frac{r_3}{\prod_{A_i\in S_2}\gamma+\tau(A_i)}}, C_3).$$

Finally, the user recovers the message

$$M = \frac{C_m}{e(g,h)^{\kappa\cdot\alpha\cdot r_2}\cdot e(g',h')^{\kappa\cdot\alpha\cdot r_3}} = \frac{C_m}{e(g,h)^{\kappa\cdot\alpha}}$$

4.4 Security Analysis

In this section, we prove that our scheme is secure against selective chosen-ciphertext attacks, assuming that the (n, s_1, s_2, t_1)-aMSE-DDH problem is hard.

Theorem 4.2. *Let λ be an integer. For any adversary $\mathcal{A}$ against the* IND-sCPA *security of our CP-ABE encryption scheme, for an attribute universe $\mathcal{P}$ of size n, and a challenge pair (s_1, s_2, t_1) with $s_1 = |S_1|, s_2 = |S_2|, 1 \leq t_1 \leq s_1$, there exists an algorithm B of the (n, s_1, s_2, t_1)-aMSE-DDH problem, such that*

$$\mathsf{Adv}_{\mathcal{B}}^{\mathsf{aMSE\text{-}DDH}}(\lambda) \geq \mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sCPA}}(\lambda).$$

Proof. We firstly discuss the high level idea of the proof. To prove the theorem, we assume that there exists an adversary $\mathcal{A}$ which can break our CP-ABE scheme with non-negligible advantage. We show how to use this adversary as a black-box to construct an algorithm $\mathcal{B}$ that breaks the (n, s_1, s_2, t_1)-augmented multi-sequence of exponents decisional Diffie-Hellman problem. The main idea in the proof will be to use the input of the (n, s_1, s_2, t_1)-aMSE-DDH problem to define the group generators with some polynomials in γ in their exponents as well as the randomness numbers so that public parameters and private keys can be simulated.

For the algorithm $\mathcal{B}$ breaking the (n, s_1, s_2, t_1)-aMSE-DDH problem, $\mathcal{B}$ is given a bilinear map group system $\mathbb{S} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(\cdot,\cdot))$, and an (n, s_1, s_2, t_1)-aMSE-DDH problem instance in $\mathbb{S}$. $\mathcal{B}$ thus have four co-prime polynomials f, g_1, g_2 and h_1 defined by the vector $\overrightarrow{x}_{2n-1-s_1+t_1} = (x_1, \ldots, x_{2n-1-s_1+t_1})$, of orders $n - s_1 - s_2$, s_1, s_2 and $n - s_1 - 1 + t_1$ respectively, and the values

$$\begin{cases}
g_0, g_0^{\gamma}, \ldots, g_0^{\gamma^{2n-s_1+t_1-3}}, \quad g_0^{\kappa\cdot\gamma\cdot f(\gamma)g_2(\gamma)}, & (4.1.1)\\
g_0^{\alpha\cdot g_2(\gamma)\cdot\gamma^0}, \ldots, g_0^{\alpha\cdot g_2(\gamma)\cdot\gamma^{n-s_1-s_2+1}}, & (4.1.2)\\
g_0^{\omega\cdot\gamma}, \ldots, g_0^{\omega\cdot\gamma^n}, & (4.1.3)\\
g_0^{\frac{\kappa\gamma f(\gamma)g_1(\gamma)}{\zeta}}, & (4.1.4)\\
g_0^{\frac{g_1(\gamma)\cdot\alpha\gamma^0}{\zeta}}, \ldots, g_0^{\frac{g_1(\gamma)\cdot\alpha\cdot\gamma^{n-s_1-s_2+1}}{\zeta}}, & (4.1.5)\\
g_0^{\frac{\omega\gamma^0}{\zeta}}, \ldots, g_0^{\frac{\omega\gamma^{n-1}}{\zeta}}, & (4.1.6)\\
h_0^{g_1(\gamma)\cdot\gamma^0}, \ldots, h_0^{g_1(\gamma)\cdot\gamma^{n+t_1-3}}, \quad h_0^{\kappa\cdot g_1^2(\gamma)h_1(\gamma)}, & (4.1.7)\\
h_0^{\alpha\cdot g_1(\gamma)\cdot\gamma^0}, \ldots, h_0^{\alpha\cdot g_1(\gamma)\cdot\gamma^{2n-1}}, & (4.1.8)\\
h_0^{\omega\cdot g_1(\gamma)\cdot\gamma^0}, \ldots, h_0^{g_1(\gamma)\cdot\omega\cdot\gamma^{n+s_1-1}}, & (4.1.9)\\
h_0^{\zeta\cdot h_1(\gamma)\cdot g_1(\gamma)\cdot\gamma^0}, \ldots, h_0^{\zeta\cdot h_1(\gamma)\cdot g_1(\gamma)\cdot\gamma^{s_2-2}}, & (4.1.10)\\
h_0^{\zeta\cdot\alpha\cdot g_2(\gamma)\cdot\gamma^0}, \ldots, h_0^{\zeta\cdot\alpha\cdot g_2(\gamma)\cdot\gamma^{2n-1}}, & (4.1.11)\\
h_0^{g_1(\gamma)\cdot\frac{\zeta\cdot h_1(\gamma)-1}{\gamma}}, \quad h_0^{\zeta\kappa g_2^2(\gamma)} & (4.1.12)
\end{cases}$$

where κ, ζ, ω, α and γ are unknown random elements of $\mathbb{Z}_p$. $\mathcal{B}$ is also given an element $T_b = e(g_0, h_0)^{\kappa\cdot f(\gamma)g_1(\gamma)g_2(\gamma)} \in \mathbb{G}_T$ and a random group element $T_{1-b} \in \mathbb{G}_T$ where b is a fair coin independent of $\mathcal{B}$'s view.

At a high level, our simulation works as follows. $\mathcal{B}$ simulates the joint distribution consisting of adversary's view in its attack in the security game, and the hidden bit β which is not a part of the adversary's view. We will show that if the input comes as $b = 0$, the simulation will be perfect, and so the adversary will launch its full ability breaking our CP-ABE. We will also show that if the input comes as $b = 1$, then the adversary's view is independent of β, and therefore the adversary's advantage is negligible. This immediately implies $\mathcal{B}$ distinguishing the distribution of its input: run the simulator and adversary together, and if the simulator outputs β and the adversary outputs β', B outputs $b' = 0$ if $\beta = \beta'$, and 1 otherwise.

We now give the details of the simulation. From now on, we will denote by W_S the subset $W \cap S$.

Init $\mathcal{B}$ defines an attribute universe $\mathcal{P} = \{A_1, \ldots, A_n\}$ of cardinal n. $\mathcal{A}$ gives $\mathcal{B}$ the challenge access structure $\mathbb{A}^*$ defined by a threshold and AND-gate policy $(S_1, t_1) \wedge (S_2)$ where $S_1, S_2 \subset \mathcal{P}$ of respective cardinal s_1, s_2 and a threshold value of cardinal $1 \leq t_1 \leq s_1$. Here, we assume $S_1 = \{A_{n-s_1-s_2+1}, \ldots, A_{n-s_2}\}$ and $S_2 = \{A_{n-s_2+1}, \ldots, A_n\}$.

Setup The algorithm $\mathcal{B}$ defines $g := g_0^{f(\gamma)\cdot g_2(\gamma)}$, $h := h_0^{g_1(\gamma)}$, $\eta := \zeta \cdot \frac{g_2(\gamma)}{g_1(\gamma)}$; thus, $g' = g^{\frac{1}{\eta}} = g_0^{\frac{f(\gamma)g_1(\gamma)}{\zeta}}$, $h' = h^{\eta} = h_0^{\zeta \cdot g_2(\gamma)}$. $\mathcal{B}$ then can compute

- the value $u = g^{\alpha\gamma} = g_0^{\alpha\gamma \cdot f(\gamma)g_2(\gamma)}$ with line (4.1.2) of its input values, since the exponent $\alpha \cdot \gamma \cdot f(\gamma)g_2(\gamma)$ is a linear combination of $\{g_2(\gamma)\cdot\alpha, \ldots, g_2(\gamma)\cdot \alpha \cdot \gamma^{n-s_1-s_2+1}\}$ and $\mathcal{B}$ knows the coefficients of the exponent polynomial.
- the value $u' = g'^{\alpha\gamma} = g_0^{\frac{\alpha\gamma \cdot f(\gamma)g_1(\gamma)}{\zeta}}$ with line (4.1.5), in the same way as computing u.
- the value $Y = e(g,h)^{\alpha} = e(g_0^{f(\gamma)g_2(\gamma)}, h_0^{g_1(\gamma)})^{\alpha} = e(g_0^{\alpha\cdot f(\gamma)g_2(\gamma)}, h_0^{g_1(\gamma)})$ with line (4.1.2) for $g_0^{\alpha\cdot f(\gamma)g_2(\gamma)}$ and line (4.1.7) for $h_0^{g_1(\gamma)}$.
- elements in $\{h^{\alpha\gamma^i} = h_0^{\alpha\cdot g_1(\gamma)\cdot\gamma^i}\}_{i=0,\ldots,2n-1}$ with line (4.1.8).
- elements in $\{h'^{\alpha\gamma^i} = h_0^{\zeta\alpha\cdot g_2(\gamma)\cdot\gamma^i}\}_{i=0,\ldots,2n-1}$ with line (4.1.11).

To complete the setup phase, $\mathcal{B}$ needs to define the encoding of attributes $\tau(A_i)$ and the values of set $\mathcal{D}$.

- The encoding τ is defined as $\tau(A_i) = x_i$ for $i = 1, \ldots, n$. It can be seen that the encodings of the first $n - s_1 - s_2$ elements are the opposite of the roots of $f(X)$, the encodings of the attributes in S_1 are the opposite of roots of $g_1(X)$, and the encodings of the attributes in S_2 are the opposite of roots of $g_2(X)$.

– The set $\mathcal{D} = \{d_1, \ldots, d_n - 1\}$ is defined as $d_i = x_{n+i}$ for $i = 1, \ldots, n-1-s_1+t_1$ following d_j for $j = n-s_1+t_1, \ldots, n-1$ is picked uniformly at random in $\mathbb{Z}_p$ repeatedly until it is distinct from $\{x_1, \ldots, x_{2n-1-s_1+t_1}, d_{n-s_1+t_1}, \ldots, d_{j-1}\}$.

We note the values of $d_1, \ldots, d_{n-1-s_1+t_1}$ are the opposite of roots of $h_1(X)$.

Finally, $\mathcal{B}$ sends to $\mathcal{A}$ the simulated public parameters:

$$\left(u, u', Y, \{h^{\alpha\gamma^i}, h'^{\alpha\gamma^i}\}_{i=0,\ldots,2n-1}, \mathcal{D}, \tau\right).$$

Phase 1 The adversary $\mathcal{A}$ makes private key queries. To respond to a query on attribute set $W \subset \mathcal{P}$, where $W \not\models \mathbb{A}^*$, the algorithm $\mathcal{B}$ must produce a tuple of the form

$$\left(\{g^{\frac{r_1}{\gamma+\tau(A_i)}}, g'^{\frac{r_3}{\gamma+\tau(A_i)}}\}_{A_i \in W}, \{h^{r_1\gamma^i}\}_{i=0,\ldots,n-2}, h^{\frac{r_1-r_2}{\gamma}}\right).$$

Observe that since $W \not\models \mathbb{A}^*$ all allowed queries must satisfy $|W_{S_1}| < t_1$ or $|W_{S_2}| < s_2$. $\mathcal{B}$ defines the polynomials for $i = 1, 2$,

$$Q_{W_{S_i}}(X) = \begin{cases} 1 & |W_{S_i}| = 0 \\ \lambda_i \cdot \prod_{A \in \omega_{S_i}} (X + \tau(A)) & |W_{S_i}| > 0 \end{cases},$$

where $\lambda_i = \left(\prod_{A \in \omega_{S_i}} \tau(A)\right)^{-1}$, and simulates a private key for W according to the following cases:

If $|W_{S_1}| < t_1$: $\mathcal{B}$ picks at random y_{1c}, y_{3c} in $\mathbb{Z}_p$, and defines

$$\begin{aligned} r_1 &:= (1 + \omega y_{1c}\gamma) Q_{W_{S_1}}(\gamma), \\ r_2 &:= 1 - \omega y_{3c}\gamma Q_{W_{S_2}}(\gamma), \\ r_3 &:= \omega y_{3c}\gamma Q_{W_{S_2}}(\gamma). \end{aligned}$$

$\mathcal{B}$ then computes the elements for sk_W:

– For any attribute $A \in W$,

$$g'^{\frac{r_3}{\gamma+\tau(A)}} = g_0^{\frac{\omega\gamma y_{3c}}{\zeta} \cdot \frac{f(\gamma) g_1(\gamma) Q_{W_{S_2}}(\gamma)}{\gamma+\tau(A)}}.$$

Since an attribute $A \in W$ must be in W_{S_2}, S_1 or $\mathcal{P} \setminus (S_1 \cup S_2)$, $(\gamma + \tau(A)) | f(\gamma) g_1(\gamma) Q_{W_{S_2}}(\gamma)$. The element can be computed with line (4.1.6) as its exponent polynomial is then a linear combination of $\{\frac{\omega}{\zeta}, \ldots, \frac{\omega\gamma^n}{\zeta}\}$ of degree at most n in γ.

– For any attribute $A \in W$,

$$g^{\frac{r_1}{\gamma+\tau(A)}} = g_0^{\omega\gamma y_{1c} \cdot \frac{f(\gamma)g_2(\gamma)Q_{W_{S_1}}(\gamma)}{\gamma+\tau(A)}} \cdot g_0^{\frac{f(\gamma)g_2(\gamma)Q_{W_{S_1}}(\gamma)}{\gamma+\tau(A)}}.$$

Since an attribute $A \in W$ can be in W_{S_1}, S_2 or $\mathcal{P} \setminus (S_1 \cup S_2)$, $(\gamma + \tau(A))|f(\gamma)g_2(\gamma)Q_{W_{S_1}}(\gamma)$. The first factor can be computed with line (4.1.3) as its exponent is a polynomial in γ of degree at most $n-1$, and the second factor can be computed with line (4.1.1) as its exponent is a polynomial in γ of degree at most $n-2$.

– The value $h^{\frac{r_1-r_2}{\gamma}} =$

$$h_0^{\omega g_1(\gamma)\cdot(y_{1c}Q_{W_{S_1}}(\gamma)+y_{3c}Q_{W_{S_2}}(\gamma))} \cdot h_0^{g_1(\gamma)\frac{Q_{W_{S_1}}(\gamma)-1}{\gamma}},$$

where the first factor can be computed from line (4.1.9) and the second factor can be computed from line (4.1.7), since $Q_{W_{S_1}}(\gamma)$ is a polynomial with independent term 1 by its definition, thus $g_1(\gamma)\frac{Q_{W_{S_1}}(\gamma)-1}{\gamma}$ is a linear combination of $\{g_1(\gamma), g_1(\gamma)\cdot\gamma, \ldots, g_1(\gamma)\cdot\gamma^{t_1-1}\}$.

– Elements in $\{h^{r_1\gamma^i}\}_{i=0,\ldots,n-2}$ can be computed as

$$h^{r_1\gamma^i} = h_0^{g_1(\gamma)\omega y_{1c}Q_{W_{S_1}}(\gamma)\cdot\gamma^{i+1}} \cdot h_0^{g_1(\gamma)Q_{W_{S_1}}(\gamma)\cdot\gamma^i}$$

where the first factor can be computed from line (4.1.9) and the second factor can be computed from line (4.1.7).

If $|W_{S_2}| < s_2$: $\mathcal{B}$ picks at random y_{1c}, y_{3c} in $\mathbb{Z}_p$, and defines

$$\begin{aligned}
r_1 &:= \omega y_{1c}\gamma Q_{W_{S_1}}(\gamma),\\
r_2 &:= 1 - \omega y_{3c}\gamma Q_{W_{S_2}}(\gamma) - \zeta\cdot h_1(\gamma)\cdot Q_{W_{S_2}}(\gamma),\\
r_3 &:= \omega y_{3c}\gamma Q_{W_{S_2}}(\gamma) + \zeta\cdot h_1(\gamma)\cdot Q_{W_{S_2}}(\gamma).
\end{aligned}$$

$\mathcal{B}$ then computes the elements for sk_W:

– For any attribute $A \in W$,

$$g'^{\frac{r_3}{\gamma+\tau(A)}} = g_0^{\frac{\omega\gamma y_{3c}}{\zeta}\cdot\frac{f(\gamma)g_1(\gamma)Q_{W_{S_2}}(\gamma)}{\gamma+\tau(A)}} \cdot g_0^{\frac{f(\gamma)Q_{W_{S_2}}(\gamma)g_1(\gamma)\cdot h_1(\gamma)}{\gamma+\tau(A)}}.$$

Since an attribute $A \in W$ must be in W_{S_2}, S_1 or $\mathcal{P} \setminus (S_1 \cup S_2)$, thus $(\gamma + \tau(A))|f(\gamma)g_1(\gamma)Q_{W_{S_2}}(\gamma)$. The first factor can be computed from line (4.1.6) as its exponent is a polynomial in γ of degree at most $n-1$, and the second factor can be computed from line (4.1.1) as its exponent

is a polynomial in γ of degree at most $2n - s_1 + t_1 - 3$.

– For attribute $A \in W$,

$$g^{\frac{r_1}{\gamma+\tau(A)}} = g_0^{\omega\gamma y_{1c} \cdot \frac{f(\gamma)g_2(\gamma)Q_{W_{S_1}}(\gamma)}{\gamma+\tau(A)}}.$$

Since an attribute $A \in W$ must be in W_{S_1}, S_2 or $\mathcal{P} \setminus (S_1 \cup S_2)$, $(\gamma + \tau(A))|f(\gamma)g_2(\gamma)Q_{W_{S_1}}(\gamma)$. It can be computed from line (4.1.3).

– Elements in $\{h^{r_1\gamma^i}\}_{i=0,\ldots,n-2}$ can be computed as

$$h^{r_1\gamma^i} = h_0^{g_1(\gamma)\omega y_{1c}Q_{W_{S_1}}(\gamma)\cdot\gamma^{i+1}},$$

which can be computed from line (4.1.9).

– Finally, $\mathcal{B}$ needs to compute the value of $h^{\frac{r_1-r_2}{\gamma}}$ from

$$\begin{cases} J_1 = h_0^{\omega g_1(\gamma)(y_{1c}Q_{W_{S_1}}(\gamma)+y_{3c}Q_{W_{S_2}}(\gamma))} \\ J_2 = h_0^{\zeta g_1(\gamma)h_1(\gamma)\frac{Q_{W_{S_2}}(\gamma)-1}{\gamma}} \\ J_3 = h_0^{g_1(\gamma)\frac{\zeta h_1(\gamma)-1}{\gamma}} \\ h^{\frac{r_1-r_2}{\gamma}} = J_1 \cdot J_2 \cdot J_3 \end{cases}$$

where J_1 can be computed from line (4.1.9); J_2 can be computed from line (4.1.10) since $\gamma|Q_{W_{S_2}}(\gamma) - 1$ by the definition of $Q_{W_{S_2}}(\gamma)$; and J_3 is given from line (4.1.12).

Challenge Once $\mathcal{A}$ sends to $\mathcal{B}$ the two messages M_0 and M_1, $\mathcal{B}$ flips a coin $\beta \in \{0, 1\}$, and sets

$$C_m^* = T_0 \cdot M_\beta.$$

To simulate the rest of the challenge ciphertext, $\mathcal{B}$ implicitly defines the randomness for the encryption as $\kappa^* = \kappa/\alpha$, and sets

$$C_2^* = h^{\kappa \cdot g_1(\gamma)h_1(\gamma)} = h_0^{\kappa \cdot g_1^2(\gamma)h_1(\gamma)}$$

which is given in line (4.1.7), and

$$C_3^* = h'^{\kappa \cdot g_2(\gamma)} = h_0{}^{\zeta \cdot \kappa \cdot g_2^2(\gamma)}$$

which is given in line (4.1.12). To complete the ciphertext, B computes

$$C_1^* = u^{-\kappa'} = g_0^{-\kappa\gamma f(\gamma)g_2(\gamma)}$$

from line (4.1.1), and

$$C_1'^* = u'^{-\kappa'} = g_0^{\frac{-\kappa\gamma f(\gamma)g_1(\gamma)}{\zeta}}$$

from line (4.1.4). $\mathcal{B}$ gives $\mathcal{A}$ the challenge ciphertext $CT^* = (C_m^*, C_1^*, C_1'^*, C_2^*, C_3^*)$.

Phase 2 After the challenge step $\mathcal{A}$ may make other key extraction queries, which are answered as before.

Guess $\mathcal{A}$ outputs a β'. If $\beta' = \beta$, $\mathcal{B}$ outputs 0; otherwise $\mathcal{B}$ outputs 1.

Perfect Simulation: When $b = 0$,

$$T_0 = e(g_0, h_0)^{\kappa \cdot f(\gamma)g_1(\gamma)g_2(\gamma)} \in \mathbb{G}_T,$$

observe the challenge ciphertext

$$\begin{aligned} C_m^* &= M_\beta \cdot e(g_0, h_0)^{\kappa \cdot f(\gamma)g_1(\gamma)g_2(\gamma)} \\ &= M_\beta \cdot e(g_0^{\alpha \cdot f(\gamma)g_1(\gamma)}, h_0^{g_2(\gamma)})^\kappa \\ &= M_\beta \cdot Y^{\kappa^*}. \end{aligned}$$

Thus, CT^* is a valid ciphertext for $\mathbb{A}^*$, and the challenge ciphertext issued by $\mathcal{B}$ comes from a distribution identical to that in the actual construction; however, we must still show that the public parameters and private keys issued by $\mathcal{B}$ are appropriately distributed. But this follows from the fact that the unknown random numbers $\gamma, \kappa, \omega, \zeta, \alpha$ are chosen uniformly random in $\mathbb{Z}_p$ as well as other group elements from the input.

Probability Analysis:
Let $\mathcal{I} = (\overrightarrow{x}_{2n-1-s_1+t_1}, \gamma, \kappa, \omega, \alpha, T_b, T_{1-b})$ be the input of the algorithm $\mathcal{B}$ and the adversary $\mathcal{A}$ break our CP-ABE scheme with advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sCPA}}(\lambda)$. If $b = 0$, then the simulation is perfect, $\mathcal{A}$ will guess the bit β correctly with its advantage, and

$$|\Pr[\mathcal{B}(\mathcal{I}) = 0 | b = 0] - \frac{1}{2}| = \mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sCPA}}(\lambda).$$

Else, $b = 1$ and T_0 is uniformly random in $\mathbb{G}_T$, thus C_m^* is uniformly random and independent in $\mathbb{G}_T$ as well. In this case, the value of β is independent from $\mathcal{A}$'s view,

$$\Pr[\mathcal{B}(\mathcal{I}) = 0 | b = 1] = \frac{1}{2}.$$

Thus, we have that

$$\begin{aligned}\mathsf{Adv}_{\mathcal{B}}^{\mathsf{aMSE\text{-}DDH}}(\lambda) &= |\Pr[\mathcal{B}(\mathcal{I})=0|b=0] - \Pr[\mathcal{B}(\mathcal{I})=0|b=1]| \\ &\geq \mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sCPA}}(\lambda).\end{aligned}$$

This concludes the proof of Theorem. □

4.5 Efficiency and Performance

In this section, some of the previous CP-ABE schemes [CZF11, EMN+09, GZC+12, HLR10, RD13b, TDM12] with constant-seize ciphertexts and our scheme are compared from the aspects of efficiency. In Table 4.1 , efficiency comparisons are made in terms of the attribute private key size and master secret key, the computation overheads of encryption and decryption and the expressiveness of access policy. All the listed CP-ABE schemes have short and constant-size ciphertexts.

Table 4.1: Comparison of CP-ABE schemes with constant-sieze ciphertexts

Scheme	sk	msk	Enc	Dec	A.P.
[EMN+09]	$2L_{\mathbb{G}_1}$	$(nm+1)L_{\mathbb{Z}_p}$	$(n+1)\mathbb{G}_1 + 2\mathbb{G}_T$	$2C_e + 2\mathbb{G}_2$	AND_m
[HLR10]	$(n+\lvert A_C\rvert -1)L_{\mathbb{G}_1}$	$L_{\mathbb{G}_1} + 2L_{\mathbb{Z}_p}$	$(2n+2\lvert A_U\rvert -4)\mathbb{G}_1 + 2\mathbb{G}_T$	$3C_e + (\lvert\omega\rvert^2+n-1)\mathbb{G}_1 + 4\mathbb{G}_T$	Threshold
[CZF11]	$(n+1)L_{\mathbb{G}_1}$	$2nL_{\mathbb{G}_1} + 2nL_{\mathbb{Z}_p}$	$(\lvert A_U\rvert +2)\mathbb{G}_1 + (n-A_U+2)\mathbb{G}_T$	$2C_e + A_C\mathbb{G}_1 + 2\mathbb{G}_T$	$\text{AND}^*_{+,-}$
[GZC+12]	$2n(n+\lvert A_U\rvert)L_{\mathbb{G}_1}$	$L_{\mathbb{Z}_p}$	$(n+\lvert A_C\rvert +3)\mathbb{G}_1 + 2\mathbb{G}_T$	$2C_e + n(n+\lvert A_C\rvert +2)\mathbb{G}_1 + 2\mathbb{G}_T$	Threshold
[TDM12]	$(n+1)L_{\mathbb{G}_1}$	$3nL_{\mathbb{Z}_p}$	$\lvert A_C\rvert C_e + \mathbb{G}_1 + 2\mathbb{G}_T$	$2C_e + n\mathbb{G}_1 + \mathbb{G}_T$	$\text{AND}^*_{+,-}$
[RD13b]	$2L_{\mathbb{G}_1}$	$2L_{\mathbb{G}_1}$	$(n+2)\mathbb{G}_1 + 2\mathbb{G}_2$	$2C_e + 2\mathbb{G}_T$	AND_m
$\mathcal{S}_{T\&A}$	$(2\lvert A_U\rvert +n)L_{\mathbb{G}_1}$	$L_{\mathbb{G}_1} + 3L_{\mathbb{Z}_p}$	$(2n+2\lvert A_C\rvert -6)\mathbb{G}_1 + 2\mathbb{G}_T$	$3C_e + (\lvert\omega\rvert^2+n-1)\mathbb{G}_1 + 5\mathbb{G}_T$	Threshold &AND

n : Total number of attributes in systems;
m : Total number of possible values of an attribute in systems;
A_C: The set of attributes included in the access policy of a ciphertext;
A_U: The set of attributes included in a user's private key;
C_e: The cost of bilinear maps;
ω: Least subset of attributes satisfying an access structure;
$\mathbb{G}_?$: Group or the cost of operation in group, for $\mathbb{G}_1$ or $\mathbb{G}_T$;
L_*: Bit length of element in *.

It can be seen that the proposed construction enjoys the advantage of the most complex access policies as well as the succinct master secret key while falls back in private key length and computational cost of decryption. In terms of computational overheads in encryption, the proposed construction is comparable to other schemes. Overall, the proposed construction achieves a new level of complexity of expressiveness and remains the efficiency in a comparable level.

4.6 Intractability of (n, s_1, s_2, t_1)-aMSE-DDH

In this section, we provide the analysis of the intractability of (n, s_1, s_2, t_1)-aMSE-DDH problem. The intractability analysis is based on the analysis in generic group

model in [DP08].

4.6.1 (n, s_1, s_2, t_1)-aMSE-DDH

In this section, we prove the intractability of distinguishing the two distributions involved in the $(n,\ s_1,\ s_2,\ t_1)$-aMSE-DDH problem (cf. Corollary 4.1, section 4.2). The proof is conducted in the generic group model: we exploit the framework of Definition 2.27 and 2.28 for the $(n,\ s_1,\ s_2,\ t_1)$-aMSE-DDH problem; we then demonstrate that the problem holds in the generic group model.

Proof of Corollary 4.1. To wrap up Corollary 4.1, we consider our problem in the weakest case $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$ and pose $\alpha = \alpha'\zeta, \omega = \omega'\zeta, \kappa = \kappa'\zeta, g_0 = g, h_0 = h^{\beta\gamma}$. Our problem can be reformulated as decisional (P, Q, F)-GDHE Problem where

$$
\begin{aligned}
P = & \left(\begin{array}{l}
1, \gamma, \ldots, \gamma^{2n-s_1+t_1-3}, \\
\kappa'\zeta \cdot \gamma \cdot f(\gamma) g_2(\gamma), \\
\zeta\alpha' \cdot \gamma^0 \cdot g_2(\gamma), \ldots, \zeta\alpha' \cdot \gamma^{n-s_1-s_2+1} \cdot g_2(\gamma), \\
\zeta\omega' \cdot \gamma, \zeta\omega' \cdot \gamma^2 \ldots, \zeta\omega' \cdot \gamma^n, \\
\kappa' \cdot \gamma \cdot f(\gamma) g_1(\gamma), \\
\alpha' \cdot \gamma^0 \cdot g_1(\gamma), \ldots, \alpha' \cdot \gamma^{n-s_1-s_2+1} \cdot g_1(\gamma), \\
\omega', \omega' \cdot \gamma, \ldots, \omega' \cdot \gamma^n, \\
\beta \cdot \gamma^1 \cdot g_1(\gamma), \ldots, \beta \cdot \gamma^{n+t_1-2} \cdot g_1(\gamma), \\
\beta\kappa'\zeta \cdot \gamma \cdot g_1^2(\gamma) h_1(\gamma) \\
\beta\alpha \cdot \gamma^1 \cdot g_1(\gamma), \ldots, \beta \cdot \alpha \cdot \gamma^{2n} \cdot g_1(\gamma) \\
\beta\omega \cdot \gamma^1 \cdot g_1(\gamma), \ldots, \beta\omega \cdot \gamma^{n+s_1} \cdot g_1(\gamma), \\
\beta\zeta \cdot \gamma^1 \cdot h_1(\gamma) g_1(\gamma), \ldots, \beta\zeta \cdot \gamma^{s_2-1} \cdot h_1(\gamma) g_1(\gamma), \\
\beta\zeta \cdot \alpha \cdot \gamma^1 \cdot g_2(\gamma), \ldots, \beta\zeta \cdot \alpha \cdot \gamma^{2n} \cdot g_2(\gamma), \\
\beta \cdot g_1(\gamma) \cdot (\zeta \cdot h_1(\gamma) - 1), \\
\beta\kappa'\zeta^2 \cdot \gamma \cdot g_2^2(\gamma)
\end{array}\right) \\
Q = & (1) \\
F = & \beta \cdot \kappa' \cdot \zeta \cdot \gamma \cdot f(\gamma) g_1(\gamma) g_2(\gamma).
\end{aligned}
$$

We need to prove the independence of F from $\langle P, Q \rangle$. By making all possible products of two polynomials from P which are multiples of $\beta \cdot \kappa'$, we want to prove

that the sum of any polynomials from the list R below does not lead to F:

$$R = \begin{cases} \beta\kappa'\zeta \cdot \gamma \cdot A_1(\gamma)g_1^2(\gamma)h_1(\gamma) \\ \beta\kappa'\zeta^2 \cdot \gamma \cdot A_2(\gamma)g_2^2(\gamma) \\ \beta\kappa'\zeta \cdot \gamma \cdot B_1(\gamma)f(\gamma)g_1(\gamma)g_2(\gamma) \\ \beta\kappa' \cdot \gamma^2 \cdot B_2(\gamma)f(\gamma)g_1^2(\gamma) \\ a_1\beta\kappa'\zeta \cdot \gamma \cdot (\zeta \cdot h_1(\gamma) - 1) \cdot f(\gamma)g_1(\gamma)g_2(\gamma) \\ a_2\beta\kappa' \cdot \gamma \cdot (\zeta \cdot h_1(\gamma) - 1) \cdot f(\gamma)g_1^2(\gamma) \\ \beta\kappa'\zeta^2 \cdot \gamma^2 \cdot C_2(\gamma)f(\gamma)g_1(\gamma)g_2(\gamma)h_1(\gamma) \\ \beta\kappa'\zeta \cdot \gamma^2 \cdot C_1(\gamma)f(\gamma)g_1^2(\gamma)h_1(\gamma) \end{cases}$$

where a_1 and a_2 are constant coefficients; A_1, A_2, B_1, B_2, C_1, C_2 are polynomials in γ.

After simplifying the list R, it can be seen that if F is not independent of $\langle P, Q\rangle$ we can then derive $\zeta \cdot \gamma \cdot f(\gamma)g_1(\gamma)g_2(\gamma)$ from following list R':

$$R' = \begin{cases} \zeta \cdot \gamma \cdot A_1(\gamma)g_1^2(\gamma)h_1(\gamma) & (4.2.1) \\ \zeta^2 \cdot \gamma \cdot A_2(\gamma)g_2^2(\gamma) & (4.2.2) \\ \zeta \cdot \gamma \cdot B_1(\gamma)f(\gamma)g_1(\gamma)g_2(\gamma) & (4.2.3) \\ \gamma^2 \cdot B_2(\gamma)f(\gamma)g_1^2(\gamma) & (4.2.4) \\ a_1\zeta \cdot \gamma \cdot (\zeta \cdot h_1(\gamma) - 1) \cdot f(\gamma)g_1(\gamma)g_2(\gamma) & (4.2.5) \\ a_2 \cdot \gamma \cdot (\zeta \cdot h_1(\gamma) - 1) \cdot f(\gamma)g_1^2(\gamma) & (4.2.6) \\ \zeta^2 \cdot \gamma^2 \cdot C_2(\gamma)f(\gamma)g_1(\gamma)g_2(\gamma)h_1(\gamma) & (4.2.7) \\ \zeta \cdot \gamma^2 \cdot C_1(\gamma)f(\gamma)g_1^2(\gamma)h_1(\gamma) & (4.2.8) \end{cases}$$

where a_1 and a_2 are constant coefficients; A_1, A_2, B_1, B_2, C_1, C_2 are polynomials in γ with $0 \leq \deg A_1, \deg A_2 \leq n - s_1 - 2 + \max(0, t_1 - s_2); 0 \leq \deg B_1, \deg B_2 \leq n + t_1 - 3; 0 \leq \deg C_1, \deg C_2 \leq s_2 - 2$.

Thus, we have the following equation:

$$\begin{aligned} \zeta \cdot \gamma \cdot f(\gamma)g_1(\gamma)g_2(\gamma) = \\ & \zeta \cdot \gamma \cdot A_1(\gamma)g_1^2(\gamma)h_1(\gamma) + \zeta^2 \cdot \gamma \cdot A_2(\gamma)g_2^2(\gamma) + \\ & \zeta \cdot \gamma \cdot B_1(\gamma)f(\gamma)g_1(\gamma)g_2(\gamma) + \gamma^2 \cdot B_2(\gamma)f(\gamma)g_1^2(\gamma) + \\ & a_1 \cdot \zeta \cdot \gamma \cdot (\zeta \cdot h_1(\gamma) - 1) \cdot f(\gamma)g_1(\gamma)g_2(\gamma) + \\ & a_2 \cdot \gamma \cdot (\zeta \cdot h_1(\gamma) - 1) \cdot f(\gamma)g_1^2(\gamma) + \\ & \zeta^2 \cdot \gamma^2 \cdot C_2(\gamma)f(\gamma)g_1(\gamma)g_2(\gamma)h_1(\gamma) + \\ & \zeta \cdot \gamma^2 \cdot C_1(\gamma)f(\gamma)g_1^2(\gamma)h_1(\gamma). \end{aligned}$$

Observing the equation, there are two conditions that must be satisfied.

1. The right hand side must have no multiple of ζ^2, concerning (4.2.2), (4.2.5) and (4.2.7).

$$\zeta^2 \cdot \gamma \left(A_2(\gamma) g_2^2(\gamma) + g_2(\gamma) \Delta (a_1 + \gamma \cdot C_2(\gamma)) \right) = 0$$

where $\Delta = g_1(\gamma) h_1(\gamma) f(\gamma)$. It then leads to

$$-(a_1 + \gamma \cdot C_2(\gamma)) \Delta = A_2(\gamma) g_2(\gamma)$$

where $\deg C_2(\gamma) = s_2 - 2$ and $\deg g_2(\gamma) = s_2$. Since g_1, h_1, f and g_2 are co-prime (Δ and g_2 are co-prime), we must have

$$g_2(\gamma) | \left(a_1 + \gamma \cdot C_2(\gamma) \right),$$

but $\deg \left(a_1 + \gamma \cdot C_2(\gamma) \right) < \deg g_2(\gamma)$. Thus,

$$a_1 + \gamma \cdot C_2(\gamma) = 0,$$

$$a_1 = C_2(\gamma) = A_2(\gamma) = 0.$$

2. The right hand side must have no multiple without ζ, concerning (4.2.4) and (4.2.6).

$$\gamma \cdot \left(\gamma \cdot B_2(\gamma) g_1^2(\gamma) f(\gamma) - a_2 \cdot g_1^2(\gamma) f(\gamma) \right) = 0$$

which leads to

$$a_2 = \gamma \cdot B_2(\gamma)$$

where $\deg B_2(\gamma) \geq 0$. Thus,

$$a_2 = B_2(\gamma) = 0.$$

The equation can then be re-written into

$$\begin{aligned} f(\gamma) g_1(\gamma) g_2(\gamma) =& A_1(\gamma) g_1^2(\gamma) h_1(\gamma) + \gamma \cdot B_1(\gamma) g_1(\gamma) g_2(\gamma) f(\gamma) \\ &+ \gamma \cdot C_1(\gamma) \cdot g_1^2(\gamma) f(\gamma) h_1(\gamma) \end{aligned}$$

Finally, we have

$$(1 - \gamma \cdot B_1(\gamma)) g_2(\gamma) f(\gamma) = (\gamma \cdot C_1(\gamma) f(\gamma) + A_1(\gamma)) g_1(\gamma) h_1(\gamma).$$

where $1 - \gamma \cdot B_1(\gamma) \neq 0$, $\deg B_1(\gamma) \leq n + t_1 - 3$, $\deg g_1(\gamma) = s_1$ and $\deg h_1(\gamma) = n - s_1 + t_1 - 1$. Since f, g_1, g_2 and h_1 are co-prime, we must have

$$g_1(\gamma)h_1(\gamma)|(1 - \gamma \cdot B_1(\gamma)).$$

However, $\deg(1 - \gamma \cdot B_1(\gamma)) < \deg g_1(\gamma)h_1(\gamma)$ will result in $1 - \gamma \cdot B_1(\gamma) = 0$, which contradicts with the fact $1 - \gamma \cdot B_1(\gamma) \neq 0$.

□

4.7 Summary

In this chapter, we proposed a flexible CP-ABE scheme supporting a threshold and AND-gate access policies which produces constant-size ciphertexts. Compared with previous CP-ABE schemes with short ciphertexts which allow access policies to be either a single AND-gate or a single threshold, our scheme can be applied in a larger number of more general situations. The proposed scheme is proven secure against selective chosen plaintext attacks in the standard model under the assumption that the newly introduced augmented Multi-Sequence of Exponents Decisional Diffie-Hellman problem is hard. The intractability of the aMSE-DDH problem is proved in the generic group model within the framework of General Diffie-Hellman Exponent problems in [BBG05].

Chapter 5

Ciphertext-Policy Attribute-Based Encryption with Key-Delegation Abuse Resistance

In ABE system, users' access privileges and their private keys are linked. When new keys can be illegally generated without the PKG the encryption system could collapse easily, even if the access privilege provided by these new keys are limited. An insightful observation is that in most existing schemes new private keys for lesser access right can be generated by (or split from) a valid private key with ease. This "property" exists in most ABE schemes and we call it "key-delegation abuse". The application of ABE system will be hindered if the property of key-delegation abuse is maliciously exploited. In this chapter, we address the "key-delegation abuse" problem in Ciphertext-policy Attribute-based Encryption systems. We introduce a new mechanism to enhance CP-ABE schemes that provide protections against this key-delegation abuse issue. We formalise the security requirements for such a property, and subsequently construct a CP-ABE scheme that satisfies the new security requirements.

5.1 Background and Scenario

"Collusion attack resistance" is a basic security requirement in CP-ABE that a user with a private key for a set W of attributes cannot generate *new* and *valid* private keys for a set W' of attributes if $W \subset W'$, even with the help from other users. An interesting question is whether the reverse is also true. Specifically, the question is: given a private key for attribute set W, can a new key for any subset $W' \subset W$ be generated? This important issue receives a very limited attention in the literature. If the answer is positive, this can lead to some undesirable situation.

To illustrate this situation, consider the following scenario. A media broadcaster (who is the trusted authority in the cryptographic setting) controls the contents to its subscribers by encrypting the contents with a CP-ABE system. Without losing generality, the contents will be encrypted with an attribute set as follows: $\{Sport, Biography, Drama, Comedy, Action, Thriller, Fantasy, Sci\text{-}Fi, Documentary, War\}$. Note that there are ten attributes in the possible set in this example. Each possible channel is sold for \$10/month, and hence, it will cost

\$100/month to subscribe to all channels. To make the package deal more attractive, the media broadcaster introduces a premium user package. For a premium user package, the user needs to subscribe to *all* channels, and hence the ten attributes, and the premium user will be granted two additional channels, namely $\{HD, Hollywood - movies\}$, and the premium price is \$100/month for the whole package. Consider the case where a malicious user, Malva, purchases the premium package. If the CP-ABE scheme that is adopted allows Malva to create a new private key for any attribute, which is a subset to the original attribute set that he has, then Malva can make money from this case. He will then construct a private key for the attribute *Sport* for example, and sells this for \$9/month, and for the ten possible attributes, he will accrue \$90/month. Additionally, he can sell any combinations of the attribute sets (such as $\{Sport, Fantasy\}$) and again sell it at a cheaper price than \$20/month. Note that in total, he will make more than \$100/month by simply re-selling a combination of these channels.

We point out that in this case, it is clear that Malva obtains an advanced control over potential subscribers by selling private keys of different subsets of attributes and managing his own groups of customers. With this kind of mischief, different from simply selling decrypted plaintexts, illegal keys are sold which can be used to decrypt existing and future ciphertexts. In fact, Malva has functioned as an illegal "trusted authority", who can cause further influence and deeper damage to the media broadcast system. From now on, we shall call this "property" in ABE as the *key-delegation abuse*, if the adversary can generate a private key for any subset without revealing his/her entire access rights. It is clear that this property is undesirable in many scenarios, as outlined above.

To the best of our knowledge, the key-delegation abuse problem in ABE systems is still not yet well explored in the literature, and hence, it becomes an inherent problem in ABE. Some existing solutions suggest embedding users' private information into their private keys. The malicious users may be wary of constructing new keys with the risk of leaking important information. On the other hand, the embedded information could be used for tracking devices or algorithms to pinpoint who illegally generated new keys. However, these approaches have two limitations: 1) they gave a deterrent solution, while users are still capable to issue new private keys; and 2) they need the constructed new key to trace who the malicious user is.

Our Techniques. We propose a CP-ABE scheme with key-delegation abuse resistance that supports AND-gate access policies. In our scheme, a private key is generated with components for all attributes from two sets of bilinear group elements based on if the attribute is owned by the user. The encryption algorithm will generate ciphertext components from two different sets of group elements the same way as key components. Thus, corresponding key and ciphertext components for all attributes

are forced into bilinear map for decryption where private keys cannot be split or combined. The scheme we proposed in this section could be also considered as a basic scheme that can be further extended to traceable CP-ABE applications. For the details of traceable CP-ABE applications please see Section 7.1.

5.1.1 Related Work

In [HJSS08], Hinek et al. mentioned the problem of *key cloning*, and another third party should be involved in each users decryption in their scheme, which makes it impractical. Then, the problem of building a secure CP-ABE supporting traceability has recently been studied in [LRK09, LHC+11, LCW13a, LCW13b]. The access policies in [LRK09, LHC+11] only support a single AND gate with wild-card. The traceable CP-ABE proposed in [LCW13b] is as fully secure, highly expressive and efficient as a conventional CP-ABE such as the one in [LOS+10], but it only supports tracing 'well-formed' illegally constructed private keys. Later, [LCW13a] proposed a new CP-ABE scheme proved fully secure which can trace not 'well-formed' illegally constructed private keys. However, traceability cannot prevent "key-delegation abuse" issue – malicious users can still illegally generate keys in private.

5.1.2 Violating Access Control Policy with "Key-Abuse" Property

The *key-delegation abuse* property is that a user who owns a private key for attribute set W can generate a new private for a subset $W' \subset W$. This property exists in majority of CP-ABE schemes. In the following, we shall demonstrate that this key-delegation abuse property can lead to some undesirable situation where the access control policy is violated.

Without losing generality, we shall consider the Cheung and Newport scheme proposed in [CN07]. Cheung and Newport proposed a CP-ABE scheme [CN07] (which is referred to as the CN scheme throughout this paper), in which access structure is restricted to an AND gate, but the i-th attribute is allowed to be either positive A_i, negative $\neg A_i$ or "don't care". In their system, let the attribute universe be $\mathcal{P} = \{A_1, A_2, A_3, A_4, A_5\}$ with size $n = 5$, then the public key is $\mathsf{params} = (\mathbb{G} = \langle g \rangle, |\mathbb{G}| = p, e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T, Y = e(g,g)^y \in \mathbb{G}_T, \{T_k = g^{t_k}, T_{n+k} = g^{t_{n+k}}, T_{2n+k} = g^{t_{2n+k}} \in \mathbb{G}\}_{A_k \in \mathcal{P}})$ where $y, \{t_k, t_{n+k}, t_{2n+k} \in \mathbb{Z}_p\}_{A_k \in \mathcal{P}}$ are picked at random uniformly, and the master secret key is $\mathsf{msk} = (y, \{t_k, t_{n+k}, t_{2n+k}\}_{A_k \in \mathcal{P}})$.

A private key for attribute set $W = \{A_1, A_2, A_3\}$ is

$$sk_W = \left(\hat{D} = g^{y-r}, \{D_i = g^{\frac{r_i}{t_i}}\}_{A_i \in W}, \{D_i = g^{\frac{r_i}{t_{n+i}}}\}_{A_i \in \mathcal{P} \setminus W}, \{F_i = g^{\frac{r_i}{t_{2n+i}}}\}_{A_i \in \mathcal{P}}\right)$$

where $r = \sum_{i=1}^{n} r_i$ and $\{r_i\}_{i=1,\ldots,n}$ are picked uniformly at random.

To encrypt a message M with AND gate access policy $\mathbb{A}_S = \bigwedge_{A_i \in S} A_i$ where $S = \{A_1, A_2\}$, we pick κ uniformly at random and then compute

$$CT = \left(\mathbb{A}_S, C_m = MY^{\kappa}, \hat{C} = g^{\kappa}, \{C_i = T_i^{\kappa}\}_{A_i \in S}, \{C_i = T_{2n+i}^{\kappa}\}_{A_i \in \mathcal{P} \setminus S}\right) .$$

To decrypt the ciphertext CT using sk_W, only several group elements of sk_W are used as

$$M = \frac{C_m}{e(\hat{C},\hat{D}) \cdot \prod_{A_i \in S} e(D_i, C_i) \prod_{A_i \in \mathcal{P} \setminus S} e(F_i, C - i)} = \frac{C_m}{e(g^s, g^{y-r}) \prod_{i=1}^{n} e(g,g)^{r_i \cdot \kappa}} = \frac{C_m}{e(g,g)^{y \cdot \kappa}} = \frac{C_m}{Y^{\kappa}}.$$

Thus, the user who owns sk_W can generate a new key

$$sk' = \left(\hat{D}' = \hat{D}, \{D_i' = D_i\}_{\{A_i\}_{i=1,2}}, \{F_i' = F_i\}_{A_i \in \mathcal{P}}\right)$$

to decrypt ciphertexts with AND gate $(A_1), (A_1 \wedge A_2), (A_2)$ since sk' includes all group elements that will be needed during the decryption algorithm.

From the example, it can be seen that to decrypt ciphertexts with different access policies, different parts of a private key are used during the decryption, which makes it plausible to illegally generate new keys. This property of key-delegation abuse does not break the security of encryption schemes and sometimes is adopted for applications like key delegation. However, unauthorised key generation can lead to violation of access control policy.

Chapter Organisation. The paper is organised as follows: Section 5.2 provides the new security model against key-delegation abuse attacks. In Section 5.3 our CP-ABE construction is presented, and the security proof is presented in Section 5.4. Finally, the chapter is summarised in Section 5.5.

5.2 Security Model against Key-delegation Abuse Attacks

We now give the security definition against Key-Delegation Abuse Attacks in CP-ABE system. This is described by a security game between a challenger and an adversary. The game is formalised based on [GLSW08] and proceeds as follows:

Setup The challenger runs the Setup algorithm and gives the public parameters params to the adversary. The attribute universe $\mathcal{P}$ and message space $\mathcal{M}$ are also defined during this step.

Queries The adversary queries the challenger for private keys corresponding to different sets of attributes $W_1, \ldots, W_q \subseteq \mathcal{P}$. In response, for each query W_j

for $1 \leq j \leq q$ the challenger runs $\mathsf{KeyGen}(\mathsf{msk}, W_j)$ to compute the private key sk_{W_j}, and send it back to the adversary $\mathcal{A}$. $\mathcal{A}$ can query the challenger adaptively.

Output The adversary chooses a new attribute set $W^* \neq W_j$ for $1 \leq j \leq q$, generates a new private key sk^* for attribute set W^*, a new general decryption algorithm $\mathsf{Dec}^*(\mathsf{params}, CT, sk)$, and send them to the challenger.

The adversary ***wins*** if

1. $\mathsf{Dec}^*(sk^*, \mathsf{Enc}(\mathsf{params}, M, \mathbb{A}) = M$ for all $\mathbb{A} = \bigwedge_{A_i \in S} A_i$, $S \subseteq W^*$ and any message $M \in \mathcal{M}$.

2. For all polynomial time decryption algorithms Dec', for all $\mathbb{A} = \bigwedge_{A_i \in S} A_i, S \not\subset W^*$ and any pair of distinct messages M_0, M_1 and uniformly random bit b, we have $Pr[\mathsf{Dec}'(sk^*, \mathsf{Enc}(\mathsf{params}, M_b, \mathbb{A})) = M_b] < 1/2 + \epsilon$, where ϵ is negligible.

The advantage of $\mathcal{A}$ is defined to be the probability that $\mathcal{A}$ wins the security game.

Definition 5.1. *A ciphertext-policy attribute-based encryption system is secure against Key-Abuse Attacks if all polynomial time adversaries have at most a negligible advantage in this security game.*

5.3 Construction

In this section, we shall present our CP-ABE scheme. For simplicity, let the universe of attributes be $\mathcal{P} := \{A_1, \ldots, A_n\}$ for some natural number n.

In our construction the key generation algorithm will link the key components of one user with a specific set of group elements, and then apply the secret sharing technology to all attributes, so that the key cannot be split or combined to obtain other valid secret keys. Each private key will be generated including one key component per attribute: if the user owns this attribute the key component will be generated with the set of group elements of t_i; otherwise, generated with the set of group elements of t_{n+i}. The encryption algorithm will take as input an AND gate and distribute a random exponent $\kappa \in \mathbb{Z}_p$ according to all attributes: if an attribute is included in the AND gate there will be only one ciphertext component for this attribute generated with the set of group elements h_i for decryption; otherwise, two ciphertext components for this attribute will be generated with h_i and h_{n+i}.

$\mathsf{Setup}(1^\lambda, \mathcal{P})$: Given a security parameter λ and an attribute universe $\mathcal{P}$ of size of n, the setup algorithm first chooses a bilinear group G of prime order p. It

then chooses random numbers $t_1, \ldots, t_{2n}, \alpha \in \mathbb{Z}_p$, random group generators $g_0, h_0 \in \mathbb{G}$, and computes

$$Y = e(g_0, h_0)^{\alpha}, h_1 = h_0^{t_1}, \ldots, h_n = h_0^{t_n}, h_{n+1} = h_0^{t_{n+1}}, \ldots, h_{2n} = h_0^{t_{2n}}.$$

The public parameters params are $\mathsf{params} = (h_1, \ldots, h_{2n}, Y, e, \mathbb{G}, \mathbb{G}_T, \mathcal{P})$. The master secret key msk is $\mathsf{msk} = (g_0, t_1, \ldots, t_{2n}, \alpha)$.

$\mathsf{Enc}(\mathsf{params}, M, \mathbb{A})$: To encrypt a message $M \in \mathbb{G}_T$ with an access structure $\mathbb{A} = \bigwedge_{A_i \in S} A_i$ the following steps are taken. A random value $\kappa \in \mathbb{Z}_p$ is picked uniformly. The ciphertext is then generated as:

$$CT = \left(\mathbb{A}, C_m = MY^{\kappa}, \{C_i = h_i^{\kappa}\}_{A_i \in S}, \{C_i = h_{n+i}^{\kappa}, C_i' = h_i^{\kappa}\}_{A_i \in \mathcal{P} \setminus S}\right).$$

$\mathsf{KeyGen}(\mathsf{msk}, W)$: To generate a private key for attribute set $W \subseteq \mathcal{P}$ the following steps are taken. $n-1$ random values $r_1, \ldots, r_{n-1}$ are randomly chosen in $\mathbb{Z}_p$ and compute $r_n = \alpha - r_1 - \cdots - r_{n-1} \in Z_p$. The private key for the attribute set W:

$$sk = \left(W, \{D_i = g_0^{\frac{r_i}{t_i}}\}_{A_i \in W}, \{D_i = g_0^{\frac{r_i}{t_{n+i}}}\}_{A_i \in \mathcal{P} \setminus W}\right).$$

$\mathsf{Dec}(\mathsf{params}, CT, sk)$: Suppose that a ciphertext, CT, is encrypted with an access structure $\mathbb{A} = \bigwedge_{A_i \in S} A_i$ and we have a private key for attribute set W, where $S \subseteq W$.

Then, the ciphertext can be decrypted by following steps:

$$\begin{aligned}
\prod_{A_i \in S \cup \{\mathcal{P} \setminus W\}} e(D_i, C_i) \prod_{A_i \in W \setminus S} e(D_i, C_i') &= \prod_{A_i \in W} e(g_0^{\frac{r_i}{t_i}}, h_i^{\kappa}) \prod_{A_i \in \mathcal{P} \setminus W} e(g_0^{\frac{r_i}{t_{n+i}}}, h_{n+i}^{\kappa}) \\
&= \prod_{A_i \in W} e(g_0^{\frac{r_i}{t_i}}, h_0^{t_i \kappa}) \prod_{A_i \in \mathcal{P} \setminus W} e(g_0^{\frac{r_i}{t_{n+i}}}, h_0^{t_{n+i} \kappa}) \\
&= e(g_0, h_0)^{\kappa \sum_{A_i \in \mathcal{P}} r_i} = e(g_0, h_0)^{\alpha \kappa}. \\
\frac{C_m}{\prod_{A_i \in S \cup \{\mathcal{P} \setminus W\}} e(D_i, C_i) \prod_{A_i \in W \setminus S} e(D_i, C_i')} &= \frac{MY^{\kappa}}{e(g_0, h_0)^{\alpha \kappa}} = M.
\end{aligned}$$

5.4 Security Analysis

We shall prove the following theorems.

Theorem 5.2. *If the DBDH assumption holds, our CP-ABE scheme defined in Section 5.3 is secure in the sense of Definition 2.22.*

Proof. To prove the theorem, let us assume that there is an adversary $\mathcal{A}$ that can break our CP-ABE scheme with non-negligible probability. We show how to use this adversary to construct an algorithm $\mathcal{B}$ which breaks the DBDH assumption.

For the algorithm $\mathcal{B}$ breaking the DBDH assumption, we let the challenger set the groups G and G_T of prime p with an efficient bilinear map, e and generator g. The challenger then flips a fair binary coin μ independent of $\mathcal{B}$'s view. If $\mu = 0$ the challenger sets $(A, B, C, Z) = (g^a, g^b, g^c, e(g, g)^{abc})$; otherwise $(A, B, C, Z) = (g^a, g^b, g^c, e(g, g)^z)$. At a high level, our simulation works as follows. We build a simulator that simulates the joint distribution consisting of adversary's view in its attack in the security game, and the hidden bit β which is not a part of the adversary's view.

We will show that if the input comes as $\mu = 0$, the simulation will be perfect, and so the adversary will launch its full ability breaking our CP-ABE. We will also show that if the input comes as $\mu = 1$, then the adversary's view is independent of β, and therefore the adversary's advantage is negligible. This immediately implies $\mathcal{B}$ distinguishing the distribution of its input tuple: run the simulator and adversary together, and if the simulator outputs β and the adversary outputs β', $\mathcal{B}$ outputs $\mu = 0$ if $\beta = \beta'$, and 1 otherwise.

We now give the details of the simulator.

The input to the simulator is $(p, G, G_T, e, g, A = g^a, B = g^b, C = g^c, Z)$.

Init During the *Init* phase, the simulator receives the challenge access structure $\mathbb{A}^* = \bigwedge_{A_i \in S^*} A_i$, where $S^* \subseteq \mathcal{P}$, from the adversary $\mathcal{A}$.

Setup First simulator chooses random numbers $\upsilon, \nu, \theta_1, \ldots, \theta_n, \gamma_1, \ldots, \gamma_n \in \mathbb{Z}_p$. Next, the simulator computes

$$
\begin{aligned}
&g_0 = g^{\upsilon}, h_0 = g^{\nu}, h_i|_{A_i \in \mathcal{P}} = g^{\nu\theta_i} = h_0^{\theta_i}, \\
&h_{n+i}|_{A_i \in W^*} = B^{\nu\gamma_i} = h_0^{b\gamma_i}, h_{n+i}|_{A_i \in \mathcal{P} \setminus W^*} = g^{\nu\gamma_i} = h_0^{\gamma_i}, \\
&Y = e(A, B)^{\upsilon\nu} = e(g_0, h_0)^{ab}.
\end{aligned}
$$

Since $h_i = h_0^{t_i}$ and $h_{n+i} = h_0^{t_{n+i}}$ for each attribute $A_i \in \mathcal{P}$, the simulator sets $t_i := \theta_i \in \mathbb{Z}_p$ for each attribute $A_i \in \mathcal{P}$, $t_{n+i} := b\gamma_i \in \mathbb{Z}_p$ for each attribute $A_i \in W^*$ and $t_{n+i} := \gamma_i \in \mathbb{Z}_N$ for each attribute $A_i \in \mathcal{P} \setminus W^*$. Since $Y = e(u_0, v_0)^{\alpha}$, the simulator also sets $\alpha := ab \in \mathbb{Z}_p$.

The simulated public parameters are $\mathsf{params} = (h_1, \ldots, h_{2n}, Y, e, G, G_T, \mathcal{P})$. The master secret key is $\mathsf{msk} = (g_0, t_1, \ldots, t_{2n}, \alpha)$.

Phase 1 The adversary $\mathcal{A}$ makes private key queries. The simulator responds to a query on W, where $S^* \not\subseteq W$, as follows. Observe that there must exist

an attribute $A_k \in S^*$ such that $k \notin W$. The simulator first chooses such an attribute k. Next, the simulator chooses $r'_1, \ldots, r'_{n-1} \in \mathbb{Z}_N$ uniformly at random and computes $r'_n = -\sum_i r'_i$. Then the simulator sets $r_i := br'_i$ for each attribute $A_i \neq k \in \mathcal{P}$ and $r_k := ab + br'_k$ for the attribute k.

Finally, the simulator computes

$$\forall A_i \in W, D_i = B^{\frac{\upsilon r'_i}{\theta_i}} = (g^\upsilon)^{\frac{br'_i}{\theta_i}} = g_0^{\frac{r_i}{t_i}}$$
$$\forall A_i \notin W, A_i \in S^*, i \neq k, D_i = g^{\frac{\upsilon r'_i}{\gamma_i}} = (g^\upsilon)^{\frac{br'_i}{b\gamma_i}} = g_0^{\frac{r_i}{t_{n+i}}}$$
$$\forall A_i \notin W, A_i \in S^*, i = k, D_k = A^{\frac{\upsilon}{\gamma_k}} \cdot g^{\frac{\upsilon r_k}{\gamma_k}} = g^{\frac{(ab+br'_k)\upsilon}{b\gamma_k}} = g_0^{\frac{r_k}{t_{n+k}}}$$
$$\forall i \notin W, i \notin S^*, D_i = B^{\frac{\upsilon r'_i}{\gamma_i}} = (g^\upsilon)^{\frac{br'_i}{\gamma_i}} = g_0^{\frac{r_i}{t_{n+i}}}$$

and passes $sk = (W, \{D_i\}_{A_i \in \mathcal{P}})$ onto $\mathcal{A}$.

Here we check the correctness of the simulated private key.

$$\sum_{A_i \in \mathcal{P}} r_i = \sum_{A_i \neq A_k, i \in \mathcal{P}} r_i + r_k = b \sum_{A_i \neq A_k, A_i \in \mathcal{P}} r'_i + ab + br'_k = ab.$$

Challenge The adversary $\mathcal{A}$ outputs messages M_0, M_1. The simulator generates a bit $\beta \in \{0, 1\}$ and sends $\mathcal{A}$ the challenge ciphertext:

$$CT^* = \Big(\mathbb{A}^*, C_m = M_\beta \cdot Z^{\upsilon\nu}, \{C_i = C^{\nu\theta_i} = {h_i}^c\}_{A_i \in S^*},$$
$$\{C_i = C^{\nu\gamma_i} = h_{n+i}^c, C'_i = C^{\nu\theta_i} = h_i^c\}_{A_i \in \mathcal{P} \setminus S^*}\Big).$$

Phase 2 $\mathcal{A}$ makes key generation queries, and the simulator responds as in Phase 1.

Guess Finally, the adversary outputs guesses β'. If $\beta = \beta'$, $\mathcal{B}$ outputs 0 indicating that $Z = e(g, g)^{abc}$; otherwise, it outputs 1.

Perfect Simulation: When $\mu = 1$ and $Z = e(g, g)^{abc}$, we have

$$C_m = M_\beta e(g, g)^{abc\upsilon\nu} = M_\beta e(g_0, h_0)^{abc} = M \cdot Y^c.$$

Thus, CT^* is a valid ciphertext for $\mathbb{A}^*$, and the public key and the challenge ciphertext issued by the simulator comes from a distribution identical to that in the actual construction; however, we still must show that the private keys issued by the simulator are appropriately distributed. To show that the keys issued by the simulator are appropriately distributed, it suffices to show that,

from A's view, the value g^a, g^b is uniformly random and independent. But this follows from the fact that g^a, g^b is chosen uniformly at random in $\mathbb{G}$ from the input.

Probability Analysis: We assume the adversary $\mathcal{A}$ breaks our CP-ABE scheme with non-negligible probability ϵ. If $Z = e(g,g)^{abc}$, then the simulation is perfect, and $\mathcal{A}$ will guess the bit β correctly with probability $1/2 + \epsilon$. Else, $Z = e(g,g)^z$ is uniformly random in $\mathbb{G}_T$, and thus C_m is uniformly random and independent element in $\mathbb{G}_T$. In this case, with probability $1 - 1/p$ the value of β is independent from $\mathcal{A}$'s view. Thus, we have that

$$\Pr[\mathcal{B}(A, B, C, Z) = 1] \geq \frac{1}{2} + \epsilon(1 - 1/p),$$

and

$$\mathsf{Adv}_{\mathcal{B}}^{\mathsf{DBDH}}(\lambda) \geq \epsilon(1 - 1/p).$$

This concludes the proof of Theorem. □

Theorem 5.3. *Our CP-ABE scheme is secure against Key-Delegation Abuse (in the sense of Definition 5.1) in the generic group model.*

Proof. To prove our scheme is secure against key-delegation abuse, the generic group model is used for conducting a simulation of the security game in Definition 5.1. We adopt the similar generic bilinear group model of [BBG05, Sho97] to show that as long as the adversary acts generically there is a negligible probability that he/she can win the security game against key-delegation abuse with our scheme. This signifies that if there exists an efficient adversary who can win the security game with our scheme, the adversary must exploit specific mathematical properties of the paring group used for implementing our construction.

Concerning the gap between the generic group model and the standard model, we believe it would be preferable to give a proof in standard model with a reduction from an adversary winning the security game with our scheme to a well-known complexity hard problem. We also believe that such reductions will only exist for more complex schemes (for specific paring groups) under a weaker security notion compared to our security game against key-delegation abuse attacks since our scheme is the first construction that meets our proposed security property.

High Level Idea

We first discuss the high level idea of the proof.

In the generic group model, the adversary can only manipulate group elements by using the canonical group operations, independent of the encoding for group elements. Thus if the adversary is given group elements $g^{\delta_1}, \ldots, g^{\delta_t} \in \mathbb{G}$ as its

only inputs, then each element of $\mathbb{G}$ output by the adversary must be of the form $g^{\pi(\delta_1,\ldots,\delta_t)}$, where π is a fixed multi-linear polynomial.

Suppose the adversary gives a new private key sk^* with a decryption algorithm $Dec^*(\cdot)$ for an attribute set W^*, with which ciphertexts encrypted with $\mathbb{A}^* = \bigwedge_{A_i \in W^*} A_i$ can be decrypted. Using a standard argument for the generic group model, we first show that if this is to happen with non-negligible probability, then the multi-linear polynomials as described above in the new private key must also satisfy corresponding constraints. Thus our approach is to assume that the multi-linear polynomials corresponding to the adversary's output satisfy the required constraints, and then obtain a contradiction. We proceed by arguing that in order to satisfy the constraints, the polynomials must have certain structure (i.e., they can only depend on certain given group elements).

First, for a ciphertext CT encrypted under $\mathbb{A}^* = \bigwedge_{A_i \in W^*} A_i$ the new private key can decrypt M from C_m if it can be used to compute $Y^\kappa = e(g_0, h_0)^{\alpha\kappa}$. Thus, it contains a group element in $\mathbb{G}$ for each attribute in $\mathcal{P}$ to pair the corresponding C_i (or C_i') in the ciphertext in bilinear map. We denote these group elements by D_i^* for attribute A_i in $\mathcal{P}$ and the necessary structure of the new private key can be presented as $(W^*, \{D_i^*\}_{A_i \in \mathcal{P}})$.

After narrowing down the necessary construction for sk^*, we note that D_i^* needs to be constructed based on key components $D_i^{(j)}$ from j-th queried private key $sk^{(j)}$ for attribute set W_j since there is no other given group elements related to the unknown master secret key α for the adversary. Nevertheless, we also note that because of the difference of the queried attribute sets, for the same attribute A_i the key components $D_i^{(j)}$ might be generated based on different sets of group elements, which makes them irreconcilable to be combined together. Thus, the new private key sk^* can only depend on one queried private key sk_j where $W^* \subset W_j$. But this will result in that $sk*$ can be used to decrypt ciphertexts encrypted with W_j that is an attribute set beyond the supposed W^*, which contradicts the second condition in the security game's definition.

Details of Proof

We consider two random encodings ψ_0, ψ_T of the additive group $\mathbb{Z}_p$ respectively, that is injective maps $\psi_0, \psi_T : \mathbb{Z}_p \to \{0,1\}^L$, where $L > 3\log(p)$. We write $\mathbb{G} = \psi_0(x) : x \in \mathbb{Z}_p$,$\mathbb{G}_T = \psi_T(x) : x \in \mathbb{Z}_p$. We are given oracles to compute the induced group action on $\mathbb{G}, \mathbb{G}_T$ and an oracle to compute a non-degenerate bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. We refer to $\mathbb{G}$ as a generic bilinear group.

We now proceed with the proof, following the standard approach for generic groups with $\psi_0, \psi_T, \mathbb{G}, \mathbb{G}_T$ defined as above. Let $g = \psi_0(1)$(we will write g^x to denote $\psi_0(x)$, and $e(g,g)^x$ to denote $\psi_T(x)$).

For any generic-group adversary, the security game against *key-delegation abuse*

is considered carried out by a simulator as follows. For each group element seen or created by the adversary, this simulator keeps track of its discrete logarithm by means of a multivariate rational functions in the following indeterminate formal variables:

$$\sum = \{\upsilon, \nu\} \cup \{t_i\}_{A_i \in \mathcal{P}} \cup \{r_i^{(j)}\}_{A_i \in \mathcal{P}, j \in [q]}.$$

The simulation also associates each group element with some rational function. For each distinct rational function in its collection, it inputs the value of the rational function to corresponding encoding ψ_0 or ψ_T and gives the result to the adversary as the encoding of that particular group element. The functions are associated with the group elements in the simulation as follows:

First, we suppose $g_0 = g^{\upsilon}, h_0 = g^{\nu}$.

- Public parameters params generated by Setup
  $\mathsf{params} = (h_1, \ldots, h_{2n}, Y)$.
  1. $\{\nu t_i\}_{A_i \in \mathcal{P}}$, representing $h_i = h_0^{t_i} = g^{\nu t_i}$.
  2. $\{\nu t_{n+i}\}_{A_i \in \mathcal{P}}$, representing $h_i = h_0^{t_{n+i}} = g^{\nu t_i}$.

- Private key components given by KeyGen. Let sk_j be the j-th queried private key for the attribute set W_j.

$$sk_j = \left(W_j, \{D_i^{(j)} = g_0^{\frac{r_i^{(j)}}{t_i}}\}_{A_i \in W}, \{D_i^{(j)} = g_0^{\frac{r_i^{(j)}}{t_{n+i}}}\}_{A_i \in \mathcal{P} \setminus W} \right)$$

  1. $\{\frac{\upsilon}{t_i} r_i^{(j)}\}_{j \in [q], A_i \in W_j}$, representing $D_i^{(j)} = g_0^{\frac{r_i^{(j)}}{t_i}}$.
  2. $\{\frac{\upsilon}{t_{n+i}} r_i^{(j)}\}_{j \in [q], A_i \in \mathcal{P} \setminus W_j}$, representing $D_i^{(j)} = g_0^{\frac{r_i^{(j)}}{t_{n+i}}}$.

We note that in the actual game, the values of the formal variables are chosen uniformly at random in $\mathbb{Z}_p$. Two distinct functions may in that case evaluate to the same value. The simulation is faithful to the standard interaction in a generic group, except in the event that two of the distinct functions evaluate to the same value on a random assignment to the formal variables. For any two distinct functions of the form listed above, the probability of this happening is at most $O(q)/p$, since the degree of distinct multivariate polynomials is at most $O(q)$. Since this probability is negligible, we ignore this case.

Now the adversary outputs a purported new private key sk^* for a new attribute set W^* with a suitable decryption algorithm $Dec^*(\cdot)$. We first observe that to decrypt a ciphertext CT encrypted with an access structure $\mathbb{A} = \bigwedge_{A_i \in S} A_i$, where S is equal to or a subset of W^*. The new private key sk^* should contain a group

element for each attribute to pair the corresponding group element C_i (or C_i') in the ciphertext in bilinear map for $Y^\kappa = e(g_0, h_0)^{\alpha\kappa}$. We denote these group elements by D_i^* and the necessary structure of the new private key can be presented as $(W^*, \{D_i^*\}_{A_i \in \mathcal{P}})$. On the other hand, as long as the new private key satisfies the winning conditions the adversary can construct the new key sk^* the way it wants to make it look different, which means the adversary can construct the new private key component D_i^* using a linear combination of the functions listed above.

Here, we note that if the adversary tries to construct D_i^* using any functions other than $D_i^{(j)}$, then using this part of D_i^* in bilinear map will result in meaningless group element in $\mathbb{G}_T$ for decryption, which also needs to be eliminated by computing it separately; since it needs to be eliminated afterwards, we do not include it in following discussion.

Without loss of general, we assume the new private key sk^* contains the following least structure for each attribute A_i:

$$\begin{aligned} D_i^* &= \pi_i(D_i^{(1)}, \ldots, D_i^{(q)}) := (D_i^{(1)})^{\beta_{i,1}} (D_i^{(2)})^{\beta_{i,2}} \cdots (D_i^{(q)})^{\beta_{i,q}} \\ &= u_0^{\frac{1}{t_i} \sum_{A_i \in W_j} \beta_{i,j} r_i^{(j)} + \frac{1}{t_{n+i}} \sum_{i \notin W_j} \beta_{i,j} r_i^{(j)}} \end{aligned}$$

where $\pi_i(D_i^{(1)}, \ldots, D_i^{(q)}) := (D_i^{(1)})^{\beta_{i,1}} (D_i^{(2)})^{\beta_{i,2}} \cdots (D_i^{(q)})^{\beta_{i,q}}$ represents a function in $\mathbb{G}$ using components $D_i^{(j)}$ from queried private keys.

Then we can represent D_i^* as $\frac{v}{t_i} \sum_{A_i \in W_j} \beta_{i,j} r_i^{(j)} + \frac{v}{t_{n+i}} \sum_{A_i \notin W_j} \beta_{i,j} r_i^{(j)}$.

To win in the game, D_i^* needs to meet following conditions:

1. $\sum_{A_i \in \mathcal{P}} \sum_{j \in [q]} \beta_{i,j} r_i^{(j)} = \alpha$.

2. $\forall A_i \in W^*, \sum_{i \notin W_j} \beta_{i,j} r_i^{(j)} = 0$.

3. $\forall A_i \notin W^*, \sum_{j \notin W_j} \beta_{i,j} r_i^{(j)} \neq 0$ and $\sum_{A_i \in W_j} \beta_{i,j} r_i^{(j)} = 0$.

The rest of our proof proceeds by assuming the new private key sk^* satisfies the conditions above, and obtaining a contradiction: that the new private key sk^* can be used to decrypt ciphertexts encrypted with a queried attribute set W_j which contradicts the second condition in the security game's definition.

Considering condition 1, $\sum_{A_i \in \mathcal{P}} \sum_{j \in [q]} \beta_{i,j} r_i^{(j)} = \alpha$. Since $\sum_i r_i^{(j)} = \alpha$ for $j \in [q]$ and $r_i^{(j)}$ is chosen uniformly at random in $\mathbb{Z}_p$, we have

$$\beta_{1,j} = \beta_{2,j} = \cdots = \beta_{n,j}.$$

We denote them by β_j.

Considering condition 2, for all $A_i \in W^*$, $\sum_{i \notin W_j} \beta_{i,j} r_i^{(j)} = \sum_{ji \notin W_j} \beta_j r_i^{(j)} = 0$.

Since $r_i^{(j)}$ is uniformly random chosen in $\mathbb{Z}_p$, it can be concluded that

$$\text{if } \exists A_i \in W^* \text{ and } i \notin W_j, \beta_j = 0$$

which is equivalent to

$$\text{if } \beta_j \neq 0, W^* \subseteq W_j.$$

Considering condition 3, for all $A_i \notin W^*, \sum_{j \notin W_j} \beta_{i,j} r_i^{(j)} = \sum_{j \notin W_j} \beta_j r_i^{(j)} \neq 0$ and $\sum_{A_i \in W_j} \beta_{i,j} r_i^{(j)} = \sum_{A_i \in W_j} \beta_j r_i^{(j)} = 0$. Since $r_i^{(j)}$ is chosen uniformly at random in $\mathbb{Z}_p$, it can be concluded that

$$\text{if } \exists i \notin W^* \text{ and } A_i \in W_j, \beta_j = 0$$

which is equivalent to

$$\text{if } \beta_j \neq 0, W_j \subseteq W^*.$$

So W^* equals to a queried attribute set W_j, which results in either the adversary cannot generate a new key as $W^* \neq W_j$ for $j \in [q]$ or the new key will be able to decrypt ciphertexts encrypted with W_j as well since only one queried private key sk_j can be used. Therefore, our assumptions cannot be true. The adversary cannot successfully generate a new private key sk^* to win the game. □

5.5 Summary

In this chapter, we investigated an important property in ABE schemes, which we call as the "key-delegation abuse". When an ABE scheme is not key-delegation abuse resistant, it means that the private keys that the users have will allow those users to generate new set of private keys without the need of the trusted authority's involvement. To be more specific, the new *derivative keys* can be generated for attribute set W' from a private key set for W, if $W' \subset W$. We outlined some potential risks in practice, and we also pointed out that the existing schemes in the literature suffer from this property in certain scenarios. It is indeed interesting that this issue has not been well studied in the literature despite its importance for the adoption of ABE in the real situation. We proposed a security notion for the key-delegation abuse property and presented a new CP-ABE scheme that is key-delegation abuse resistant. We proved the security of the scheme in both of standard selective CPA model and the proposed model against key-delegation abuse. The proposed scheme is constructed in a succinct form, but it produces long ciphertexts, of which the size grows linearly with the total number of attributes, and requires extra computational overheads in encryption and decryption compared to other

efficient schemes that support AND-gate access policies.

Chapter 6

Ciphertext-Policy Attribute Based Encryption Supporting Access Policy Update

In many occasions, the enforced access control on encrypted data needs be updated and the original encryptor might be required to re-encrypt the message, which is impractical, since the encryptor might be unavailable. Unfortunately, to date this issue about access policy update in ABE has not been considered, which implicitly restricts the adoption of ABE in practice. In this chapter, the problem of efficiently update existing access policies on ciphertexts is focused on, and ideally this process of access policy update should not involve any further re-encryption. A new notion of ciphertext-policy attribute-based encryption supporting access policy update (CP-ABE-APU) is introduced, which enables adding attributes to and revoking attributes from existing access policies. We formalise the security requirements for this notion, and subsequently construct two provably secure CP-ABE schemes supporting AND-gate access policy with constant-size ciphertexts for user decryption.

6.1 Background and Scenario

Attribute-based encryption enforces encrypted data to be decrypted with a secure access control mechanism that the assigned attributes must satisfy the access policies associated with ciphertexts or private keys. When a message needs to be securely distributed to a range of specific recipients, it will be encrypted with an access policy that can be only satisfied by targeted recipients. The ciphertext can then be uploaded to the storage server for recipients to download and decrypt. The storage server does not need to be trusted by receivers but it functions as a proxy, which performs the task that is assigned a priori. Unfortunately, to date, the access policy enforced with the ciphertext cannot be changed once the encryption process is completed. There is no CP-ABE scheme that supports modification of access policies of ciphertexts. On the contrary, this has become a highly desirable feature as situation can change from time to time, and without the ability to update the access policy, CP-ABE may no longer be suitable in many practical scenarios. Hence, an efficient update mechanism over access policies of ciphertexts must be enabled.

One may think that the above question can be solved trivially by requesting

encryptors to re-encrypt the messages when the access policies need to be updated. However, several physical restrictions could make this approach impractical and unusable. For example, encryptors may not be available when the update is needed or encryptors may have no access to sufficient computation power or network bandwidth to accomplish the re-encryption.

Alternatively, one may think an attribute-based proxy re-encryption (AB-PRE) system can be employed for access policy update. A ciphertext-policy attribute-based proxy re-encryption (CP-AB-PRE) works as showed in Fig. 6.1. When the access policies of a certain range of ciphertexts need to be updated, re-encryption keys, one for each ciphertext, will be generated. Each re-encryption key is generated by a user private key for a specific requirement that is from the old access policy to a new access policy. The user private key used for re-encryption generation needs to satisfy the old access policy. When all the re-encryption keys are generated, they will be uploaded to a proxy. To re-encrypt a ciphertext, the proxy first checks if the old access policy of the corresponding re-encryption key matches the access policy of the ciphertext. If it is a match, the proxy then proceeds with the re-encryption.

Much effort have been put into developing and enhancing AB-PRE including CP-AB-PRE. What AB-PRE provides is an efficient mechanism of re-encryption, to wit to output the result of decrypting and encrypting to a new access policy without actually decrypting the ciphertext or knowing the plaintext.

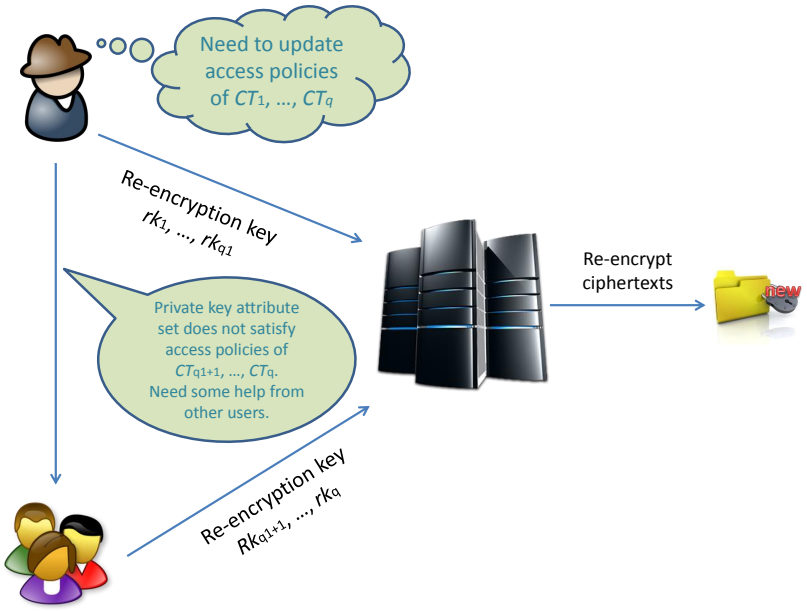

Figure 6.1: An example of user updating access policies of ciphertexts employing PRE

Nevertheless, AB-PRE does not provide an efficient access policy update mechanism not to mention the within restriction that a valid re-encryption key needs to

be generated when there is a need of access policy update. In real-world scenario the amount of ciphertexts that need to be updated rises, which leads to a difficult situation when an authority tries to generate all the re-encryption keys and then uploads them. In addition, the authority does not necessarily own a private key that satisfies the old access policies of all the involved ciphertexts. Help from other authorities or the original encryptors will be needed, which then leads to further sophisticated situations. It can be seen that to update access policies for a certain amount of ciphertexts will exceeds the capability of AB-PRE who specialises in re-encryption.

6.1.1 Overview

In this chapter, we aim to equip the notion of Attribute-based Encryption with access policy update. We present the notion of Ciphertext-policy Attribute Based Encryption supporting Access Policy Update. In our setting, the encryptor will produce encrypted data together with components used for access policy update and send them to a third party, which provides distributed storage servers and functions as access policy update proxy. This third party does not need to be trusted; it will store encrypted data for users accessing and execute access policy update algorithm as requested, which does not give it the ability of decrypting any ciphertexts. We present a new security model to capture these requirements, together with two constructions supporting AND-gate access policy provably secure under augmented assumptions. In our CP-ABE-APU constructions, a long version of ciphertext that includes a short version will be sent to storage server when a message is encrypted. The short version consists of 3 group elements and will be later downloaded by users for decryption. The long version consists of the short version as well as several extra group elements for the attribute addition and revocation: $n - s - 1$ group elements for attribute addition where n represents the total number of attributes and s represents the number of attributes contained in the AND-aget access policy; t group elements for attribute revocation, where t represents the maximum allowed number of attributes for revocation (Table 6.1). The components for access policy update will only be stored in storage servers, which makes the ciphertext sent to users for decryption of constant size of 3. We also present the proofs of security of our constructions as well as proofs of intractability of augmented assumptions.

Table 6.1: Comparison of two constructions supporting access policy update

Scheme	Update operation	Attr. universe	Attr. in policy/ Max. revocation	Ciphertext for user	Ciphertext for server
$\mathcal{S}_{AA}$	Addition	n	s	3	$n - s + 2$
$\mathcal{S}_{AR}$	Revocation	n	t	3	$t + 3$

6.1.2 Related Work

The proxy re-encryption scheme was first formalised by Blaze, Bleumer, and Strauss [BBS98]. With the concept of ABE and PRE combined, Liang et al. [LCLS09] proposed the first CP-AB-PRE scheme based on the CP-ABE scheme [OSW07] supporting non-monotonic access structures. Then Luo et al. [LHC10] proposed another CP-AB-PRE scheme with multi-value positive attributes. Aside from this, Seo et al. [SK12] proposed a CP-AB-PRE scheme which has constant paring operation latency. Liang et al. constructed CP-AB-PRE schemes [LFSW13, LAS$^+$14, LAL$^+$15] proven secure in CCA security model.

Recently, Susilo et al. [SCG$^+$16] introduced a new notion of recipient-revocable identity-based broadcast encryption scheme. In their scheme, the encryptor produces and sends ciphertexts to a proxy for broadcasting, which will also be able to revoke some identities from the original set of recipients without the knowledge the plaintext.

Chapter Organisation. The chapter is organised as follows. In Section 6.2, we present some definitions related to CP-ABE supporting Access Policy Update mechanism and augmented complexity assumption that are used. We present our CP-ABE scheme that supports attribute addition in Section 6.3, together with its security analysis. Section 6.4 deals with CP-ABE that supports attribute revocation, as well as its security analysis. Section 6.5 gives a detailed comparison and discussion about proposed schemes regarding efficiency and performance. We presented the analysis of the intractability of the hard problem that is used to analyse our schemes in Section 6.6. The analysis is provided in the generic group model. Finally, the chapter is summarised in Section 6.7.

6.2 Definitions

In this section, we provide definitions for newly proposed notions.

6.2.1 CP-ABE supporting Access Policy Update Definition

A ciphertext-policy attribute-based encryption system supporting attribute addition consists of five algorithms: Setup, Encrypt, KeyGen, Update and Decrypt.

$\mathsf{Setup}(1^\lambda, \mathcal{P})$**.** The setup algorithm takes input the attribute universe $\mathcal{P}$ as well as the implicit security parameter. It outputs the public parameters params and a master secret key msk.

$\mathsf{Enc}(\mathsf{params}, M, \mathbb{A})$**.** The encryption algorithm takes in the public parameters params, the message M, and an access structure $\mathbb{A}$ over the universe of attributes. It

will output a ciphertext CT such that only users whose private keys associated with attribute sets which satisfy the access structure $\mathbb{A}$ can decrypt M. It will also outputs a ciphertext CT_{p} that will be restored in proxy server for access policy updates. We assume that the ciphertexts implicitly contains $\mathbb{A}$.

KeyGen(msk, W). The key generation algorithm takes as input the master secret msk and a set of attributes W. It outputs a private key sk associated with W.

Update(params, CT_{p}, *opt*, $\mathcal{U}$). The addition algorithm takes as input the public parameters params, a ciphertext CT for an access policy $\mathbb{A} = \bigwedge_{A_i \in S} A$, an operation indicator *opt* = Add or Revoke and a set of attributes $\mathcal{U}$ with $\mathcal{U} \cap S = \emptyset$ if *opt* = Add or $\mathcal{U} \subset S$ if *opt* = Revoke. It outputs a new ciphertext CT' for the new access policy $\mathbb{A}' = \bigwedge_{A_i \in S \cup \mathcal{U}}$ or $\bigwedge_{A_i \in S \setminus \mathcal{U}}$ according to *opt*.

Dec(params, CT, sk). The decryption algorithm takes as input the public parameters PK, a ciphertext CT for an access structure $\mathbb{A}$, and a private key sk associated with a set of attributes W. If the attribute set W satisfies the access structure $\mathbb{A}$ then the algorithm will decrypt the ciphertext and return a message M.

6.2.1.1 Selective CPA Security Model for CP-ABE supporting Access policy Update.

We now give the security definition for CP-ABE system – Indistinguishability under selective chosen plaintext attacks. This is described by a security game between a challenger and an adversary for a security parameter $\lambda \in \mathbb{N}$. The game proceeds as follows:

Init The challenger defines an attribute universe $\mathcal{P}$ of size n and gives it to the adversary $\mathcal{A}$. $\mathcal{A}$ chooses a challenge access structure $\mathbb{A}^*$ of one attribute set $S \subset \mathcal{P}$ with $s = |S|$, and gives it to the challenger.

Setup The challenger runs the Setup algorithm and gives the public parameters params to the adversary.

Phase 1 The adversary queries the challenger for private keys corresponding to sets of attributes $W_1, \ldots, W_{q_1}$ with the restriction that none of these satisfies the access policy $\mathbb{A}^*$.

Challenge The adversary declares two equal length messages M_0 and M_1 as well as a attribute set $\mathcal{U}^*$ with $t = |\mathcal{U}^*|$ and $\mathcal{U}^* \subset S$ or $\mathcal{U}^* \cap S = \emptyset$ according to "*opt*" = Add or "*opt*"= Revoke respectively. The challenger flips a random coin $\beta \in \{0, 1\}$, and encrypts M_β with $\mathbb{A}' = \bigwedge_{A_i \in S \setminus \mathcal{U}^*} A$ for "*opt*"= Add or $\mathbb{A}' =$

$\bigwedge_{A_i \in S \cup \mathcal{U}^*} A$ for "*opt*"= Revoke, producing $CT^* = \mathsf{Enc}(\mathsf{params}, \mathbb{A}^*, M_\beta)$. It gives $CT' = CT^*$ to the adversary if $\mathcal{U}^* = \emptyset$, otherwise $CT' = \mathsf{Update}(\mathsf{params}, CT^*, opt, \mathcal{U}^*)$.

Phase 2 The adversary queries the challenger for private keys corresponding to sets of attributes $W_{q_1+1}, \ldots, W_q$ with the same restriction that none of these satisfies the access policy $\mathbb{A}^*$.

Guess The adversary outputs a guess β' for β.

The advantage of an adversary in winning this game is defined to be

$$\mathsf{Adv}^{\mathsf{IND\text{-}sCPA}}_{\mathcal{A},\mathsf{CP\text{-}ABE\text{-}APU}} = |\Pr[\beta' = \beta] - \frac{1}{2}|.$$

Definition 6.1. *A ciphertext-policy attribute-based encryption system supporting access policy update is selective chosen-plaintext attacks secure if all polynomial time adversaries have at most a negligible advantage in this security game.*

It is worth noticing that our newly defined security model has two different types of adversaries considered.

1. When $\mathcal{U}^* = \emptyset$, the challenge ciphertext CT^* is the direct result of encryption algorithm without any involvement of access policy update algorithm. It can be seen that this is essentially the property of IND-sCPA security for CP-ABE schemes that an adversary who does not hold a private key associated with a set of attributes satisfying the challenge access policy cannot distinguish which submitted message was encrypted as the challenge ciphertext.

2. When $\mathcal{U}^* \neq \emptyset$, the challenge ciphertext CT' is the result of updating $\mathcal{U}^*$ from $\mathbb{A}'$ of the ciphertext of encrypted M_β. It can be seen that in this situation it prevents the type of adversaries who obtain private keys associated with any attributes satisfying access policy before update from learning anything about the plaintext.

6.2.2 Complexity Assumption

Our construction will make use of groups with bilinear maps [BF01b], and two new computational assumptions, that fit into the General Diffie-Hellman Exponent framework proposed by Boneh, Boyen and Goh [BBG05].

The security of our schemes are reduced to the hardness of a problem, which we called the *augmented multi-sequence of exponents decisional Diffie-Hellman problem*. The problems are modified from the (l, m, t)-aMSE-DDH problem defined in [HLR10], of which the generic complexity is covered by the general Diffie-Hellman

exponent theorem due to Boneh et al. [BBG05], as the problem lies in the scope of their framework.

First we introduce the assumption which our CP-ABE-AA scheme is reduced to. Let $\mathbb{S} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(\cdot,\cdot))$ be a bilinear map group system. Let g_0 be a generator of $\mathbb{G}_1$ and h_0 be a generator of $\mathbb{G}_2$. Let n, s be two integers. The first (n, s)-*augmented multi-sequence of exponents decisional Diffie-Hellman* ((n, s)-*aMSE-DDH*$_A$) *problem* related to $\mathbb{S}$ is as follows:

Input The vector $\overrightarrow{x}_n = (x_1, \ldots, x_n)$ defines the co-prime polynomials, of which the components are pairwise distinct elements of $\mathbb{Z}_p$,

$$f(X) = \prod_{i=1}^{n-s}(X + x_i), \quad g(X) = \prod_{i=n-s+1}^{n}(X + x_i),$$

the values

$$\begin{cases} g_0, g_0^{\gamma}, \ldots, g_0^{\gamma^{n-2}}, \quad g_0^{\kappa\cdot\gamma\cdot f(\gamma)}, & (6.1.1)\\ g_0^{\alpha}, g_0^{\alpha\cdot\gamma}, \ldots, g_0^{\alpha\cdot\gamma^{n-s+1}}, & (6.1.2)\\ g_0^{\omega\cdot\gamma}, \ldots, g_0^{\omega\cdot\gamma^{n-1}}, & (6.1.3)\\ h_0, h_0^{\gamma}, \ldots, h_0^{\gamma^{s-2}}, & (6.1.4)\\ h_0^{\kappa\cdot g(\gamma)}, h_0^{\kappa\cdot\gamma\cdot g(\gamma)}, \ldots, h_0^{\kappa\cdot\gamma^{n-s}\cdot g(\gamma)}, & (6.1.5)\\ h_0^{\alpha}, h_0^{\alpha\cdot\gamma}, \ldots, h_0^{\alpha\cdot\gamma^{n}}, & (6.1.6)\\ h_0^{\omega}, h_0^{\omega\cdot\gamma}, \ldots, h_0^{\omega\cdot\gamma^{s-1}}, & (6.1.7) \end{cases}$$

where κ,ω, α, γ are unknown random elements of $\mathbb{Z}_p$, an element $T_b = e(g_0, h_0)^{\kappa\cdot f(\gamma)} \in \mathbb{G}_T$ and a random group element $T_{1-b} \in \mathbb{G}_T$ while b is a fair coin.

Output a bit b'. The problem is correctly solved if the output is $b' = b$.

The following statement is a corollary of Theorem 2.30. It provides an intractability bound in the generic model, but in groups equipped with pairings. We emphasise on the fact that, whereas the assumption has several parameters, it is non-interactive, and thus easily falsifiable [Nao03].

Corollary 6.2 (Generic Security)**.** *For any probabilistic algorithm $\mathcal{B}$ that makes at most q_G queries to the oracles performing group operations in $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ and the bilinear map $e(\cdot,\cdot)$, its advantage in solving (n, s)-aMSE-DDH$_A$ problem is bounded as*

$$\mathsf{Adv}_{\mathcal{B}}^{(n,s)\text{-}\mathsf{aMSE\text{-}DDH}_A}(\lambda) \leq \frac{(q_G + 5n + 3)^2 \cdot d}{2p}$$

where $d = 2n$.

Second, we introduce the assumption for our CP-ABE-AR scheme. Let $\mathbb{S} = (p,$ $\mathbb{G}_1,$ $\mathbb{G}_2,$ $\mathbb{G}_T,$ $e(\cdot,\cdot))$ be a bilinear map group system. Let g_0 be a generator of $\mathbb{G}_1$

and h_0 be a generator of $\mathbb{G}_2$. Let n, s be two integers. The second (n, s)-*augmented multi-sequence of exponents decisional Diffie-Hellman* ((n, s)-*aMSE-DDH*$_B$) *problem* related to $\mathbb{S}$ is as follows:

Input The vector $\overrightarrow{x}_n = (x_1, \ldots, x_n)$ defines the co-prime polynomials, of which the components are pairwise distinct elements of $\mathbb{Z}_p$,

$$f(X) = \prod_{i=1}^{n-s}(X + x_i), \quad g(X) = \prod_{i=n-s+1}^{n}(X + x_i),$$

the values

$$\begin{cases} g_0, g_0^{\gamma}, \ldots, g_0^{\gamma^{n-2}}, \quad g_0^{\kappa\cdot\gamma\cdot f(\gamma)}, & (6.2.1) \\ g_0^{\alpha}, g_0^{\alpha\cdot\gamma}, \ldots, g_0^{\alpha\cdot\gamma^{2n-s}}, & (6.2.2) \\ g_0^{\omega\cdot\gamma}, \ldots, g_0^{\omega\cdot\gamma^{n-1}}, & (6.2.3) \\ h_0, h_0^{\gamma}, \ldots, h_0^{\gamma^{s-2}}, & (6.2.4) \\ h_0^{\kappa\cdot g(\gamma)}, & (6.2.5) \\ h_0^{\alpha}, h_0^{\alpha\cdot\gamma}, \ldots, h_0^{\alpha\cdot\gamma^{n}}, & (6.2.6) \\ h_0^{\omega}, h_0^{\omega\cdot\gamma}, \ldots, h_0^{\omega\cdot\gamma^{s-1}}, & (6.2.7) \end{cases}$$

where κ, ω, α, γ are unknown random elements of $\mathbb{Z}_p$, element $T_b = e(g_0, h_0)^{\kappa\cdot f(\gamma)} \in \mathbb{G}_T$ and a random group element $T_{1-b} \in \mathbb{G}_T$ while b is a fair coin.

Output a bit b'. The problem is correctly solved if the output is $b' = b$.

Corollary 6.3 (Generic Security)**.** *For any probabilistic algorithm $\mathcal{B}$ that makes at most q_G queries to the oracles performing group operations in $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ and the bilinear map $e(\cdot, \cdot)$, its advantage in solving (n, s)-aMSE-DDH$_B$ problem is bounded as*

$$\mathsf{Adv}_{\mathcal{B}}^{(n,s)\text{-}\mathsf{aMSE}\text{-}\mathsf{DDH}_B}(\lambda) \leq \frac{(q_G + 5n + s + 4)^2 \cdot d}{2p}$$

where $d = 2(2n - s)$.

Full proofs of the intractability of Corollary 6.2 and 6.3 is given in Section 6.6.1.

6.3 Attribute Addition Construction

In this section, we shall present our ciphertext-policy attribute-based encryption scheme that supports access policy update with operation indicator $opt = \mathsf{Add}$. This construction also adopts the algorithm Aggregate introduced in Section 4.3.

6.3.1 Description

$\mathsf{Setup}(1^\lambda, \mathcal{U})$ The PKG chooses a suitable encoding τ sending each attribute in $\mathcal{U}$ onto (different) elements $\tau(A_i) = \delta \in \mathbb{Z}_p$. It also chooses a bilinear group system $\mathbb{S} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(\cdot,\cdot))$. It picks at random two generators g of $\mathbb{G}_1$ and h of $\mathbb{G}_2$. Then, the PKG picks at random $\alpha, \gamma \in \mathbb{Z}_p$ and sets $u = g^{\alpha\gamma}$, and $Y = e(g^\alpha, h)$.

The master secret key is then $\mathsf{msk} = (g, \alpha, \gamma)$ and the public parameters are

$$\mathsf{params} = \left(\mathcal{U}, n, u, Y, h, \{h^{\alpha\gamma^i}\}_{i=0,\ldots,n}, \tau\right).$$

$\mathsf{KeyGen}(\mathsf{params}, W, \mathsf{msk})$ Given any subset $W \subset \mathcal{U}$ of attributes, the PKG picks $r \in \mathbb{Z}_p$ at random, computes $sk_W = \left(\{g^{\frac{r}{\gamma+\tau(A_i)}}\}_{A_i \in W}, h^{\frac{r-1}{\gamma}}\right)$.

$\mathsf{Enc}(\mathsf{params}, M, \mathbb{A})$ Given an AND-gate access structure of a set of attributes $S \subset \mathcal{U}$ with $s = |S|$, and a message $M \in \mathbb{G}_T$, the sender picks at random $\kappa \in \mathbb{Z}_p$ and computes

$$\begin{cases} E_0 = h^{\kappa\cdot\alpha\cdot\prod_{A_i\in S}(\gamma+\tau(A_i))}, E_1 = E_0^\gamma, \ldots, E_{n-s} = E_{n-s-1}^\gamma \\ C_1 = u^{-\kappa}, \\ C_m = Y^\kappa \cdot M \end{cases}$$

The ciphertext sent from its encryptor to the storage server is then $CT_{\mathsf{p}} = (E_0, \ldots, E_{n-s}, C_1, C_m)$ while the part of $CT = (E_0, C_1, C_m)$ will be accessed by users for decryption.

$\mathsf{Update}(\mathsf{params}, CT, \text{“}\mathsf{add}\text{”}, \mathcal{U})$ Given a ciphertext CT with an AND-gate access structure of attribute set S and a set of attributes $\mathcal{U} = \{A'_1, \ldots, A'_t\}$ with $t = |\mathcal{U}|$ and $\mathcal{U} \cap S = \emptyset$, the proxy adds attributes in $\mathcal{U}$ to the AND-gate access structure of the ciphtertext CT as follows.

Let $F(x)$ be the polynomial in x as $F(x) = \prod_{A'_i\in\mathcal{U}}(x+\tau(A'_i)) = f_t x^t + f_{t-1}x^{t-1} + \cdots + f_0$.

Compute $E'_0 = E_0^{F(\gamma)} = \prod_{i=0}^t E_i^{f_i}$. Then a new ciphertext is then $CT' = (E'_0, C_1, C_m)$ with its AND-gate access structure $\mathbb{A}'$ of attribute set $S \cup \mathcal{U}$.

$\mathsf{Dec}(\mathsf{params}, CT, sk_W)$ Any user with a set of attributes W such that $W \models \mathbb{A}$ can use the private key to decrypt the ciphertext.

First, the user computes $e(g,h)^{\kappa\cdot\alpha\cdot r}$ as follows. The user computes

$$\mathsf{Aggregate}(\{g^{\frac{r}{\gamma+\tau(A_i)}}, \tau(A_i)\}_{A_i\in S}) = g^{\frac{r}{\prod_{A_i\in S_1}\gamma+\tau(A_i)}}.$$

With the output the user then computes $e(g,h)^{\kappa\cdot\alpha\cdot r} = e(g^{\frac{r}{\prod_{A_i\in S_1}\gamma+\tau(A_i)}}, E_0)$. After that, the user computes $e(g,h)^{\kappa\cdot\alpha} = e(C_1, h^{\frac{r-1}{\gamma}})\cdot e(g,h)^{\kappa\cdot\alpha\cdot r}$. Finally, the user recovers the message $M = \frac{C_m}{e(g,h)^{\kappa\cdot\alpha}}$.

6.3.2 Security Analysis

In this section, we are going to prove that our CP-ABE-AA scheme is secure against selective chosen ciphertext attacks, assuming that the (n,s)-aMSE-DDH$_A$ problem is hard to solve.

Theorem 6.4. *Let λ be an integer. For any adversary $\mathcal{A}$ against the* IND-sCPA *security of our CP-ABE-AA encryption scheme $\mathcal{S}_{AA}$, for an attribute universe $\mathcal{P}$ of size n, and a challenge set S with $s = |S|$, there exists an algorithm B of the (n,s)-aMSE-DDH$_A$ problem, such that*

$$\mathsf{Adv}_{\mathcal{B}}^{(n,s)\text{-aMSE-DDH}_A}(\lambda) \geq \mathsf{Adv}_{\mathcal{A},\mathcal{S}_{AA}}^{\text{IND-sCPA}}(\lambda).$$

Proof. We now give the details of the simulation. From now on, we will denote by W_S the subset $W \cap S$.

Init $\mathcal{B}$ defines an attribute universe $\mathcal{P} = \{A_1, \ldots, A_n\}$ of cardinal n. $\mathcal{A}$ gives $\mathcal{B}$ the challenge access structure $\mathbb{A}^*$ defined by an AND-gate policy $\bigwedge_{A_i\in S} A_i$ where $S \subset \mathcal{U}$ of respective cardinal s. Here we assume $S = \{A_{n-s+1}, \ldots, A_n\}$.

Setup The algorithm $\mathcal{B}$ defines $g := g_0^{f(\gamma)}$, $h := h_0$. $\mathcal{B}$ then can compute

- the value $u = g^{\alpha\gamma} = g_0^{\alpha\gamma\cdot f(\gamma)}$ with line (6.1.2) of its input values, since the exponent $\alpha\cdot\gamma\cdot f(\gamma)$ is a linear combination of $\{\alpha, \alpha\cdot\gamma, \ldots, \alpha\cdot\gamma^{n-s+1}\}$ and $\mathcal{B}$ knows the coefficients of the exponent polynomial;
- the value $Y = e(g,h)^{\alpha} = e(g_0^{\alpha\cdot f(\gamma)}, h_0)$ with line (6.1.2) and line (6.1.4);
- elements in $\{h^{\alpha\gamma^i} = h_0^{\alpha\cdot\gamma^i}\}_{i=0,\ldots,n}$ with line (6.1.6);
- the encoding τ is defined as $\tau(A_i) = x_i$ for $i = 1, \ldots, n$. It can be seen that the encodings of the first $n-s$ elements are the opposite of the roots of $f(X)$, the encodings of the attributes in S are the opposite of roots of $g(X)$.

Finally, $\mathcal{B}$ sends to $\mathcal{A}$ the simulated public parameters: $\left(u, Y, h, \{h^{\alpha\gamma^i}\}_{i=0,\ldots,n}, \tau\right)$.

Phase 1 The adversary $\mathcal{A}$ makes private key queries. To respond to a query on attribute set $W \subset \mathcal{U}$, where $W \not\models \mathbb{A}^*$, the algorithm $\mathcal{B}$ must produce a tuple of the form $\left(\{g^{\frac{r}{\gamma+\tau(A_i)}}\}_{A_i\in W}, h^{\frac{r-1}{\gamma}}\right)$.

Observe that since $W \not\models \mathbb{A}^*$ all allowed queries must satisfy $|W_S| < s$. $\mathcal{B}$ defines the polynomial $Q_{W_S}(X) = \begin{cases} 1 & |W_S| = 0 \\ \lambda_i \cdot \prod_{A_i \in W_S}(X + \tau(A_i)) & |W_S| > 0 \end{cases}$, where $\lambda = \left(\prod_{A \in W_S} \tau(A_i)\right)^{-1}$, and simulates a private key for W as follows:

$\mathcal{B}$ picks at random y_W in $\mathbb{Z}_p$, and defines $r := (1 + \omega y_W \gamma) Q_{W_S}(\gamma)$. $\mathcal{B}$ then computes the elements for sk_W:

- For any attribute $A_i \in W$, $g^{\frac{r}{\gamma+\tau(A_i)}} = g_0^{\omega\gamma y_W \cdot \frac{f(\gamma)Q_{W_S}(\gamma)}{\gamma+\tau(A_i)}} \cdot g_0^{\frac{f(\gamma)Q_{W_S}(\gamma)}{\gamma+\tau(A_i)}}$. Since an attribute $A_i \in W$ can be in W_S or $\mathcal{U} \setminus S$, $(\gamma + \tau(A_i)) | f(\gamma) Q_{W_S}(\gamma)$. The first factor can be computed with line (6.1.3) as its exponent is a polynomial in γ of degree at most $n-1$, and the second factor can be computed with line (6.1.1) as its exponent is a polynomial in γ of degree at most $n-2$;
- The value $h^{\frac{r-1}{\gamma}} = h_0^{\omega y_W Q_{W_S}(\gamma)} \cdot h_0^{\frac{Q_{W_S}(\gamma)-1}{\gamma}}$, where the first factor can be computed from line (6.1.7) and the second factor can be computed from line (6.1.4), since $Q_{W_S}(\gamma)$ is a polynomial with independent term 1 by its definition, thus $\frac{Q_{W_S}(\gamma)-1}{\gamma}$ is a linear combination of $\{1, \gamma, \ldots, \gamma^{s-2}\}$.

Challenge Once $\mathcal{A}$ sends to $\mathcal{B}$ the two messages M_0 and M_1 as well as an update attribute set $\mathcal{U}^*$, $\mathcal{B}$ flips a coin $\beta \in \{0, 1\}$, and sets $C_m^* = T_b \cdot M_\beta$. To simulate the rest of the challenge ciphertext, $\mathcal{B}$ implicitly defines the randomness for the encryption as $\kappa^* = \kappa/\alpha$, and sets $E_0^* = h^{\kappa^* \alpha \cdot g(\gamma)} = h_0^{\kappa \cdot g(\gamma)}$ which is given in line (6.1.5) as well as $E_1^*, \ldots, E_{n-s}^*$. To complete the ciphertext, B computes $C_1^* = u^{-\kappa^*} = g_0^{-\kappa\gamma f(\gamma)}$ from line (6.1.1). $\mathcal{B}$ gives $\mathcal{A}$ the challenge ciphertext $CT^* = (E_0^*, E_1^*, \ldots, E_{n-s}^*, C_1^*, C_m^*)$.

Phase 2 After the challenge step $\mathcal{A}$ may make other key extraction queries, which are answered as before.

Guess $\mathcal{A}$ outputs a β'. If $\beta' = \beta$, $\mathcal{B}$ outputs 0; otherwise $\mathcal{B}$ outputs 1.

Probability Analysis: Let $\mathcal{I} = (\overrightarrow{x}_n, \gamma, \kappa, \omega, \alpha, T_b, T_{1-b})$ be the input of the algorithm $\mathcal{B}$ and the adversary $\mathcal{A}$ break our CP-ABE scheme with advantage $\mathsf{Adv}^{\mathsf{IND\text{-}sCPA}}_{\mathcal{A},\mathcal{S}_{AA}}(\lambda)$. Below we analyse the simulation in two cases.

Case 1 : $\mathcal{U}^* = \emptyset$

Let $\kappa = \kappa^* \cdot \alpha$. One can verify that in this case, $E_0^* = h_0^{\kappa \cdot g(\gamma)} = h^{\kappa^* \cdot \alpha \cdot \prod_{A_i \in S}(\gamma + \tau(A_i))}$ and $C_1^* = g_0^{-\kappa \cdot \gamma \cdot f(\gamma)} = g_0^{-\kappa^* \cdot \alpha \cdot \gamma \cdot f(\gamma)} = u^{-\kappa^*}$. As for the C_m^*, we also note that if $b = 0$, $T_b = e(g_0, h_0)^{\kappa f(\gamma)}$, then $C_m^* = e(g_0, h_0)^{\kappa f(\gamma)} \cdot M_\beta = e(g^\alpha, h)^{\kappa^*} \cdot M_\beta = Y^{\kappa^*} \cdot M_\beta$. Therefore, the simulation of $\mathcal{B}$ is perfect, and the adversary $\mathcal{A}$ will

guess the bit β with its advantage. Hence, if $b = 0$ we have

$$|\Pr[\mathcal{B}(\mathcal{I}) = 0|b = 0] - \frac{1}{2}| = \mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sCPA}}(\lambda).$$

Else, if $b = 1$ and T_b is uniformly random in $\mathbb{G}_T$, C_m^* is uniformly random and independent in $\mathbb{G}_T$, and the value of β is independent from $\mathcal{A}$'s view as well,

$$\Pr[\mathcal{B}(\mathcal{I}) = 0|b = 1] = \frac{1}{2}.$$

Thus, we have the advantage of $\mathcal{B}$ in solving the (n, s)-aMSE-DDH$_B$ problem in Case 1 is

$$\begin{aligned}\mathsf{Adv}_{\mathcal{B}}^{(n,s)-\mathsf{aMSE\text{-}DDH_A}}(\lambda) &= |\Pr[\mathcal{B}(\mathcal{I}) = 0|b = 0] - \Pr[\mathcal{B}(\mathcal{I}) = 0|b = 1]| \\ &\geq \mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sCPA}}(\lambda).\end{aligned}$$

Case 2 : $\mathcal{U}^* = \{A'_1, A'_2, \ldots, A'_t\} \neq \emptyset$

In this case, we first show that how a challenge ciphertext should be produced in a real game. Formally, the correct procedures are as follows.

Let $S' = S \setminus \mathcal{U}^*$. The encryption algorithm $\mathsf{Enc}(\mathsf{params}, \mathbb{A}' = \bigwedge_{A_i \in S'} A, M_\beta)$ is run to get CT^*. More precisely, it picks a randomness $\kappa' \in \mathbb{Z}_p$ and computes,

$$\begin{aligned}CT^* &= (E_0^*, E_1^*, \cdots, E_{n-s+t}^*, C_1^*, C_m^*) \\ &= (h^{\kappa' \cdot \alpha \cdot \prod_{A_i \in S'}(\gamma + \tau(A_i))}, \ldots, h^{\kappa' \cdot \alpha \cdot \gamma^{n-s+t} \cdot \prod_{A_i \in S'}(\gamma + \tau(A_i))}, u^{-\kappa'}, Y^{\kappa'} \cdot M).\end{aligned}$$

The Addition algorithm $\mathsf{Update}(\mathsf{params}, CT^*, \text{“}\mathsf{add}\text{”}, \mathcal{U})$ is run to add the attribute set $\mathcal{U}^*$ to the access policy of the ciphertext CT^*. It processes as follows.

Let $F^*(x)$ be the polynomial in x as $F^*(x) = \prod_{A'_i \in \mathcal{U}^*}(x + \tau(A'_i)) = f_t^* x^t + f_{t-1}^* x^{t-1} + \cdots + f_0^*$. Compute $E_0'^* = (E_0^*)^{F^*(\gamma)} = \prod_{i=0}^{t}(E_i^*)^{f_i^*}$. Finally, the challenge ciphertext in a real game is produced $CT' = (E_0'^*, C_1^*, C_m^*)$.

Now we assume that the randomness κ' used in producing CT^* is defined as $\kappa' \cdot \alpha = \kappa$. The challenge ciphertext CT' turns out to be as follows,

$$C_m^* = M_\beta \cdot Y^{\kappa'} = M_\beta \cdot Y^{\frac{\kappa}{\alpha}},$$

$$E_0'^* = h^{\kappa' \cdot \alpha \cdot \prod_{A_i \in S}(\gamma + \tau(A_i))} = h^{\kappa \cdot \prod_{A_i \in S}(\gamma + \tau(A_i))} = h_0^{\kappa \cdot g(\gamma)},$$

$$C_1^* = u^{-\kappa'} = g_0^{\kappa \cdot \gamma \cdot f(\gamma)}.$$

It can be seen that if $b = 0$, $T_b = e(g_0, h_0)^{\kappa \cdot f(\gamma)}$, the challenge ciphertext in

a real game is exactly the same as the simulated challenge ciphertext. The simulated game would be a perfect simulation if it can be proved that the setting of κ' is indistinguishable from a real random value from the view of $\mathcal{A}$. It will suffice as κ is random to $\mathcal{A}$. Thus, if $b = 0$ we have

$$|\Pr[\mathcal{B}(\mathcal{I}) = 0|b = 0] - \frac{1}{2}| = \mathsf{Adv}^{\mathsf{IND\text{-}sCPA}}_{\mathcal{A},\mathcal{S}_{AA}}(\lambda).$$

On the other hand, if $b = 1$ and T_b is a random element from $\mathbb{G}_T$, C^*_m is random and independent from the view of $\mathcal{A}$,

$$\Pr[\mathcal{B}(\mathcal{I}) = 0|b = 1] = \frac{1}{2}.$$

Thus, we have the advantage of $\mathcal{B}$ in solving the (n, s)-aMSE-DDH$_B$ problem in Case 2 is

$$\begin{aligned}\mathsf{Adv}^{\mathsf{(n,s)-aMSE\text{-}DDH_A}}_{\mathcal{B}}(\lambda) &= |\Pr[\mathcal{B}(\mathcal{I}) = 0|b = 0] - \Pr[\mathcal{B}(\mathcal{I}) = 0|b = 1]| \\ &\geq \mathsf{Adv}^{\mathsf{IND\text{-}sCPA}}_{\mathcal{A},\mathcal{S}_{AA}}(\lambda).\end{aligned}$$

This completes the proof. □

6.4 Access Policy Attribute Revocation Construction

In this section, we shall present our ciphertext-policy attribute-based encryption scheme that supports access policy update with operation indicator *opt* = Revoke.

6.4.1 Description

Setup$(1^\lambda, \mathcal{U})$ The PKG selects a suitable encoding τ sending each attribute in $\mathcal{U}$ onto different elements $\tau(A_i) = \delta \in \mathbb{Z}_p$. It also chooses a bilinear group system $\mathbb{S} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(\cdot, \cdot))$. It picks at random two generators g of $\mathbb{G}_1$ and h of $\mathbb{G}_2$. Then, the PKG picks at random $\alpha, \gamma \in \mathbb{Z}_p$ and sets $\{u_i = g^{\alpha\gamma^i}\}_{i=1\ldots n}$, and $Y = e(g^\alpha, h)$.

The master secret key is then $\mathsf{msk} = (g, \alpha, \gamma)$ and the public parameters are

$$\mathsf{params} = \left(\mathcal{U}, n, \{u_i\}_{i=1,\ldots,n}, Y, h, \{h^{\alpha\gamma^i}\}_{i=0,\ldots,n}, \tau\right).$$

KeyGen$(\mathsf{params}, W, \mathsf{msk})$ Given any subset $W \subset \mathcal{P}$ of attributes, the PKG picks $r \in \mathbb{Z}_p$ at random, computes $sk_W = \left(\{g^{\frac{r}{\gamma+\tau(A_i)}}\}_{A_i \in W}, h^{\frac{r-1}{\gamma}}\right)$.

$\mathsf{Enc}(\mathsf{params}, M, \mathbb{A}, l)$ Given an AND-gate access structure of a set of attributes $S \subset \mathcal{U}$ with $s = |S|$, a message $M \in \mathbb{G}_T$ and an extra input which is a maximum revocation number $l \leq s$, the sender picks at random $\kappa \in \mathbb{Z}_p$ and computes

$$\begin{cases} E_0 = h^{\kappa \cdot \alpha \cdot \prod_{A_i \in S}(\gamma + \tau(A_i))} \\ C_1 = u_1^{-\kappa}, \ldots, C_{l+1} = u_{l+1}^{-\kappa}, \\ C_m = Y^{\kappa} \cdot M \end{cases}$$

The ciphertext sent from its encryptor to the storage server is then $CT_{\mathsf{server}} = (E_0, C_1, \ldots, C_{t+1}, C_m)$ while the part of $CT = (E_0, C_1, C_m)$ will be access by users for decryption.

$\mathsf{Update}(\mathsf{params}, CT, \text{“}\mathsf{revoke}\text{”}, \mathcal{U})$ Given a ciphertext $CT = (E_0, C_1, \ldots, C_{t+1}, C_m)$ for an AND-gate access structure $\mathbb{A} = \wedge_{A_i \in S} A$, a revocation attribute set $\mathcal{U} = \{A'_1, \ldots, A'_t\} \subseteq S$ with $t \leq l$ and the public parameters params, the revocation update algorithm works as follows.

Let $F(x)$ be the polynomial in x as

$$F(x) = \frac{1}{\prod_{A'_i \in \mathcal{U}} \tau(A'_i)} \prod_{A'_i \in \mathcal{U}} (x + \tau(A'_i)) = f_t x^t + f_{t-1} x^{t-1} + \cdots + f_0.$$

Compute

- $C'_m = C_m \cdot e(\prod_{i=1}^{t} C_i^{-f_i}, h) = M \cdot e(g^{\kappa \cdot \alpha \cdot \sum_{i=0}^{t} f_i \gamma^i}, h) = M \cdot Y^{\kappa \cdot F(\gamma)}$,
- $E'_0 = E_0^{\frac{1}{\prod_{A'_i \in \mathcal{U}} \tau(A'_i)}} = h^{\kappa \cdot \alpha \cdot \prod_{A_i \in S \setminus \mathcal{U}} (\gamma + \tau(A_i)) \cdot F(\gamma)}$,
- $C'_1 = \prod_{i=1}^{t+1} C_i^{f_{i-1}} = g^{-\kappa \cdot \alpha \cdot \gamma \cdot F(\gamma)} = u_1^{-\kappa \cdot F(\gamma)}$.

The new ciphertext is then $CT = (E'_0, C'_1, C'_m)$ with new randomness $\kappa \cdot F(\gamma)$.

$\mathsf{Dec}(\mathsf{params}, CT, sk_W)$ Any user with a set of attributes W such that $W \models \mathbb{A}$ can use the private key to decrypt the ciphertext.

First, the user computes $e(g, h)^{\kappa \cdot \alpha \cdot r}$ as follows. The user computes

$$\mathsf{Aggregate}(\{g^{\frac{r}{\gamma + \tau(A_i)}}, \tau(A_i)\}_{A_i \in S_1}) = g^{\frac{r}{\prod_{A_i \in S_1} \gamma + \tau(A_i)}}.$$

With the output the user computes $e(g, h)^{\kappa \cdot \alpha \cdot r} = e(g^{\frac{r}{\prod_{A_i \in S_1} \gamma + \tau(A_i)}}, E_0)$. After that, the user computes $e(g, h)^{\kappa \cdot \alpha} = e(C_1, h^{\frac{r-1}{\gamma}}) \cdot e(g, h)^{\kappa \cdot \alpha \cdot r}$. Finally, the user recovers the message $M = \frac{C_m}{e(g,h)^{\kappa \cdot \alpha}}$.

6.4.2 Security Analysis

In this section, we prove that our scheme is secure against selective chosen ciphertext attacks, assuming that the (n, s)-aMSE-DDH$_B$ problem is hard to solve.

Theorem 6.5. *Let λ be an integer. For any adversary $\mathcal{A}$ against the* IND-sCPA *security of our CP-ABE-AR encryption scheme $\mathcal{S}_{AR}$, for an attribute universe $\mathcal{P}$ of size n, and a challenge set$S$ with $s = |S|$, there exists an algorithm B of the (n, s)-aMSE-DDH$_B$ problem, such that*

$$\mathsf{Adv}_{\mathcal{B}}^{(n,s)\text{-aMSE-DDH}_B}(\lambda) \geq \mathsf{Adv}_{\mathcal{A},\mathcal{S}_{AR}}^{\mathsf{IND\text{-}sCPA}}(\lambda).$$

Proof. We now give the details of the simulation.

Init $\mathcal{B}$ defines an attribute universe $\mathcal{P} = \{A_1, \ldots, A_n\}$ of cardinal n. $\mathcal{A}$ gives $\mathcal{B}$ the challenge access structure $\mathbb{A}^*$ defined by an AND-gate policy $\bigwedge_{A_i \in S} A$ where $S \subset \mathcal{U}$ of respective cardinal s. Here we assume $S = \{A_{n-s+1}, \ldots, A_n\}$.

Setup The algorithm $\mathcal{B}$ defines $g := g_0^{f(\gamma)}$, $h := h_0$. $\mathcal{B}$ then can compute

- the values $u_i = g^{\alpha\gamma^i} = g_0^{\alpha\gamma^i \cdot f(\gamma)}$ with line (6.2.2) of its input values, since the exponent $\alpha \cdot \gamma^i \cdot f(\gamma)$ is a linear combination of $\{\alpha, \ldots, \alpha \cdot \gamma^{2n-s}\}$ and $\mathcal{B}$ knows the coefficients of the exponent polynomial;
- the value $Y = e(g, h)^\alpha = e(g_0^{\alpha \cdot f(\gamma)}, h_0)$ with line (6.2.2) for $g_0^{\alpha \cdot f(\gamma)}$ and line (6.2.4) for h_0;
- elements in $\{h^{\alpha\gamma^i} = h_0^{\alpha \cdot \gamma^i}\}_{i=0,\ldots,n}$ with line (6.2.6).
- the encoding τ is defined as $\tau(A_i) = x_i$ for $i = 1, \ldots, n$. It can be seen that the encodings of the first $n - s$ elements are the opposite of the roots of $f(X)$, the encodings of the attributes in S are the opposite of roots of $g(X)$.

Finally, $\mathcal{B}$ sends to $\mathcal{A}$ the simulated public parameters: $\left(u, Y, h, \{h^{\alpha\gamma^i}\}_{i=0,\ldots,n}, \tau\right)$.

Phase 1 The adversary $\mathcal{A}$ makes private key queries. To respond to a query on attribute set $W \subset \mathcal{U}$, where $W \not\models \mathbb{A}^*$, the algorithm $\mathcal{B}$ must produce a tuple of the form $\left(\{g^{\frac{r}{\gamma+\tau(A_i)}}\}_{A_i \in W}, h^{\frac{r-1}{\gamma}}\right)$.

Observe that since $W \not\models \mathbb{A}^*$ all allowed queries must satisfy $|W_S| < s$. $\mathcal{B}$ defines the polynomial $Q_{W_S}(X) = \begin{cases} 1 & |W_S| = 0 \\ \lambda_i \cdot \prod_{A_i \in W_S}(X + \tau(A_i)) & |W_S| > 0 \end{cases}$, where $\lambda = \left(\prod_{A_i \in W_S} \tau(A_i)\right)^{-1}$, and simulates a private key for W as follows:

$\mathcal{B}$ picks at random y_W in $\mathbb{Z}_p$, and defines $r := (1 + \omega y_W \gamma) Q_{W_S}(\gamma)$. $\mathcal{B}$ then computes the elements for sk_W:

– For any attribute $A_i \in W$, $g^{\frac{r}{\gamma+\tau(A_i)}} = g_0^{\omega\gamma y_W \cdot \frac{f(\gamma)Q_{W_S}(\gamma)}{\gamma+\tau(A_i)}} \cdot g_0^{\frac{f(\gamma)Q_{W_S}(\gamma)}{\gamma+\tau(A_i)}}$. Since an attribute $A_i \in W$ can be in W_S or $\mathcal{U} \setminus (S)$, $(\gamma + \tau(A_i))|f(\gamma)Q_{W_S}(\gamma)$. The first factor can be computed with line (6.2.3) as its exponent is a polynomial in γ of degree at most $n-1$, and the second factor can be computed with line (6.2.1) as its exponent is a polynomial in γ of degree at most $n-2$.

– The value $h^{\frac{r-1}{\gamma}} = h_0^{\omega y_W Q_{W_S}(\gamma)} \cdot h_0^{\frac{Q_{W_S}(\gamma)-1}{\gamma}}$, where the first factor can be computed from line (6.2.7) and the second factor can be computed from line (6.2.4), since $Q_{W_{S_1}}(\gamma)$ is a polynomial with independent term 1 by its definition, thus $\frac{Q_{W_S}(\gamma)-1}{\gamma}$ is a linear combination of $\{1, \gamma, \ldots, \gamma^{s-2}\}$.

Challenge Once $\mathcal{A}$ sends to $\mathcal{B}$ the two messages M_0 and M_1 as well as a attribute set $\mathcal{U}^*$ with $t = |\mathcal{U}^*|$ and $\mathcal{U}^* \cap S = \emptyset$ including all attributes needed to be revoked, $\mathcal{B}$ flips a coin $\beta \in \{0,1\}$, and sets $C_m^* = T_b \cdot M_\beta$. To simulate the rest of the ciphertext components, $\mathcal{B}$ sets $E_0^* = h_0^{\kappa \cdot g(\gamma)}$ which is given in line (6.2.5). Then, B computes $C_1^* = (g_0^{\kappa\gamma f(\gamma)})^{-1}$ from line (6.2.1). $\mathcal{B}$ gives $\mathcal{A}$ the challenge ciphertext $CT^* = (E_0^*, C_1^*, C_m^*)$.

Here we observe that

if $\mathcal{U}^* = \emptyset$, $t = 0$ $\mathcal{B}$ should output to the adversary $CT = \mathsf{Enc}(\mathsf{params}, \mathbb{A}^*, 0, M_\beta) = (E_0, C_1, C_m)$ for access structure $\mathbb{A}^*$, of which the challenge ciphertext matches the form;

if $\mathcal{U}^* \neq \emptyset$ $\mathcal{B}$ should output $CT' = \mathsf{Revoke}(\mathsf{params}, \mathsf{Enc}(\mathsf{params}, \mathbb{A}', t, M_\beta), \mathcal{U}^*) = (E_0', C_1', C_m)$ for access structure $\mathbb{A}^*$, of which the challenge ciphertext matches the form as well.

Phase 2 After the challenge step $\mathcal{A}$ may make other key extraction queries, which are answered as before.

Guess $\mathcal{A}$ outputs a β'. If $\beta' = \beta$, $\mathcal{B}$ outputs 0; otherwise $\mathcal{B}$ outputs 1.

Probability Analysis: Let $\mathcal{I} = (\overrightarrow{x_n}, \gamma, \kappa, \omega, \alpha, T_b, T_{1-b})$ be the input of the algorithm $\mathcal{B}$ and the adversary $\mathcal{A}$ break our CP-ABE scheme with advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sCPA}}(\lambda)$. Below we analyse the simulation in two cases.

Case 1 : $\mathcal{U}^* = \emptyset$

Let $\kappa^* = \kappa/\alpha$. One can verify that in this case, $E_0^* = h_0^{\kappa \cdot g(\gamma)} = h^{\kappa^* \cdot \alpha \cdot \gamma \cdot \prod_{A_i \in S}(\gamma+\tau(A_i))}$ and $C_1^* = g_0^{-\kappa \cdot \gamma \cdot f(\gamma)} = g_0^{-\kappa^* \cdot \alpha \cdot \gamma \cdot f(\gamma)} = u_1^{-\kappa^*}$. As for the C_m^*, we also note that if $b = 0$, $T_b = e(g_0, h_0)^{\kappa f(\gamma)}$, then $C_m^* = e(g_0, h_0)^{\kappa f(\gamma)} \cdot M_\beta = e(g^\alpha, h)^{\kappa^*} \cdot M_\beta =$

$Y^{\kappa^*} \cdot M_\beta$. Therefore, the simulation of $\mathcal{B}$ is perfect, and the adversary $\mathcal{A}$ will guess the bit β with its advantage. Hence, if $b = 0$ we have

$$|\Pr[\mathcal{B}(\mathcal{I}) = 0|b = 0] - \frac{1}{2}| = \mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sCPA}}(\lambda).$$

Else, if $b = 1$ and T_b is uniformly random in $\mathbb{G}_T$, C_m^* is uniformly random and independent in $\mathbb{G}_T$, and the value of β is independent from $\mathcal{A}$'s view as well,

$$\Pr[\mathcal{B}(\mathcal{I}) = 0|b = 1] = \frac{1}{2}.$$

Thus, we have the advantage of $\mathcal{B}$ in solving the (n, s)-aMSE-DDH$_B$ problem in Case 1 is

$$\begin{aligned}\mathsf{Adv}_{\mathcal{B}}^{\mathsf{(n,s)-aMSE\text{-}DDH_B}}(\lambda) &= |\Pr[\mathcal{B}(\mathcal{I}) = 0|b = 0] - \Pr[\mathcal{B}(\mathcal{I}) = 0|b = 1]| \\ &\geq \mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sCPA}}(\lambda).\end{aligned}$$

Case 2 : $\mathcal{U}^* \neq \emptyset$

In this case, we first show how a challenge ciphertext should be produced in a real game. Formally, the correct procedures are as follows.

Let $S' = \mathcal{U}^* \cup S$. The encryption algorithm $\mathsf{Enc}(\mathsf{params}, \mathbb{A}' = \bigwedge_{A_i \in S'} A, t, M_\beta)$ is run to get CT^*. More precisely, it picks a randomness $\kappa' \in \mathbb{Z}_p$ and computes,

$$\begin{aligned}CT^* &= (E_0^*, C_1^*, \cdots, C_{t+1}^*, C_m^*) \\ &= (h^{\kappa' \cdot \alpha \cdot \prod_{A_i \in S_1}(\gamma + \tau(A_i))}, u_1^{-\kappa'}, \ldots, u_{t+1}^{-\kappa'}, C_m = Y^{\kappa'} \cdot M).\end{aligned}$$

The revocation algorithm $\mathsf{Revoke}(\mathsf{params}, CT^*, \mathcal{U}^*)$ is run to revoke the attribute set $\mathcal{U}^*$ from the access policy of the ciphertext CT^*. It processes as follows.

Let $F(x)$ be the polynomial in x as

$$F(x) = \frac{1}{\prod_{A_i' \in \mathcal{U}^*} \tau(A_i')} \prod_{A_i' \in \mathcal{U}^*} (x + \tau(A_i')) = f_t x^t + f_{t-1} x^{t-1} + \cdots + f_0.$$

Compute $C_m' = C_m \cdot e(\prod_{i=1}^{l} C_i^{f_i}, h) = M_\beta \cdot Y^{\kappa' \cdot F(\gamma)}$.

Compute $E_0' = E_0^{\frac{1}{\prod_{A_i' \in \mathcal{U}} \tau(A_i')}} = h^{\kappa' \cdot \alpha \cdot F(\gamma) \cdot \prod_{A_i \in S}(\gamma + \tau(A_i))}$.

Compute $C_1' = \prod_{i=1}^{l+1} C_i^{f_{i-1}} = u_1^{-\kappa' \cdot F(\gamma)}$.

Finally, the challenge ciphertext in a real game is produced $CT' = (E_0', C_1', C_m')$.

Now we assume that the randomness κ' used in producing CT^* is defined as $\kappa' = \frac{\kappa}{\alpha} \cdot \frac{1}{F(\gamma)}$. Then let $\kappa^* = \kappa/\alpha$ and the challenge ciphertext CT' turns out to be as follows,

$$C'_m = M_\beta \cdot Y^{\frac{\kappa}{\alpha}} = M_\beta \cdot Y^{\kappa^*},$$

$$E'_0 = h^{\kappa \cdot \prod_{A_i \in S}(\gamma + \tau(A_i))} = h^{\kappa^* \cdot \alpha \cdot \gamma \cdot \prod_{A_i \in S}(\gamma + \tau(A_i))},$$

$$C'_1 = u_1^{\frac{-\kappa}{\alpha}} = u_1^{\kappa^*}.$$

It can be seen that if $b = 0$, $T_b = e(g_0, h_0)^{\kappa \cdot f(\gamma)}$, the challenge ciphertext in a real game is exactly the same as the simulated challenge ciphertext. The simulated game would be a perfect simulation if it can be proved that the setting of κ' is indistinguishable from a real random value from the view of $\mathcal{A}$. It will suffice as κ is random to $\mathcal{A}$. Thus, if $b = 0$ we have

$$|\Pr[\mathcal{B}(\mathcal{I}) = 0 | b = 0] - \frac{1}{2}| = \mathsf{Adv}^{\mathsf{IND\text{-}sCPA}}_{\mathcal{A},\mathcal{S}_{AR}}(\lambda).$$

On the other hand, if $b = 1$ and T_b is a random element from $\mathbb{G}_T$, C^*_m is random and independent from the view of $\mathcal{A}$, $\Pr[\mathcal{B}(\mathcal{I}) = 0 | b = 1] = \frac{1}{2}$. Thus, we have the advantage of $\mathcal{B}$ in solving the (n, s)-aMSE-DDH$_B$ problem in Case 2 is

$$\begin{aligned}\mathsf{Adv}^{(n,s)-\mathsf{aMSE\text{-}DDH_B}}_{\mathcal{B}}(\lambda) &= |\Pr[\mathcal{B}(\mathcal{I}) = 0 | b = 0] - \Pr[\mathcal{B}(\mathcal{I}) = 0 | b = 1]| \\ &\geq \mathsf{Adv}^{\mathsf{IND\text{-}sCPA}}_{\mathcal{A},\mathcal{S}_{AR}}(\lambda).\end{aligned}$$

This completes the proof. □

6.5 Comparison and Discussion

In this section, some of the previous CP-AB-PRE schemes [LCLS09, LHC10, LAS+14] and our schemes are compared from the aspects of performance and functionality. In Table 6.2 , general efficiency comparisons are made in terms of the public key size, the private key size, the ciphertext size and the computation overheads of re-encryption or update.

Although our proposed schemes have different applicable scenarios, they share a same functionality with CP-AB-PRE schemes which is to modify the access policy of a ciphertext. Compared with CP-AB-PRE, a significant difference is that our proposed schemes do not require a re-encryption key to modify access policies, which makes them less relied on encryptor personnel and resources of computation or communication. On the other hand, advanced CP-AB-PRE schemes can support

Table 6.2: Comparison to CP-AB-PRE schemes

Scheme	params	sk	CT in server	ReEnc/Update
[LCLS09]	$\mathcal{O}(n) \cdot L_{\mathbb{G}_1}$	$\mathcal{O}(n) \cdot L_{\mathbb{G}_1}$	$\mathcal{O}(n) \cdot L_{\mathbb{G}_1}$	$\mathcal{O}(n) \cdot C_e$
[LHC10]	$\mathcal{O}(n^2) \cdot L_{\mathbb{G}_1}$	$\mathcal{O}(n) \cdot L_{\mathbb{G}_1}$	$\mathcal{O}(n) \cdot L_{\mathbb{G}_1}$	$\mathcal{O}(n) \cdot C_e$
[LAS+14]	$\mathcal{O}(n) \cdot L_{\mathbb{G}_1}$	$\mathcal{O}(\lvert A_U \rvert) \cdot L_{\mathbb{G}_1}$	$\mathcal{O}(\lvert A_C \rvert) \cdot L_{\mathbb{G}_1}$	$\mathcal{O}(\lvert A_U \rvert) \cdot C_e + \mathcal{O}(\lvert A_U \rvert) \cdot \mathbb{G}$
$\mathcal{S}_{AA}$	$\mathcal{O}(n) \cdot L_{\mathbb{G}_1}$	$\mathcal{O}(\lvert A_U \rvert) \cdot L_{\mathbb{G}_1}$	$\mathcal{O}(n - \lvert A_C \rvert) \cdot L_{\mathbb{G}_1}$	$\mathcal{O}(\lvert A_M \rvert) \cdot \mathbb{G}$
$\mathcal{S}_{AR}$	$\mathcal{O}(n) \cdot L_{\mathbb{G}_1}$	$\mathcal{O}(\lvert A_U \rvert) \cdot L_{\mathbb{G}_1}$	$\mathcal{O}(\lvert A_C \rvert) \cdot L_{\mathbb{G}_1}$	$\mathcal{O}(\lvert A_M \rvert) \cdot \mathbb{G}$

n : Total number of attributes in systems;
A_C: The set of attributes included in the access policy of a ciphertext;
A_U: The set of attributes included in a user's private key;
A_M: The set of attributes requested for addition or revocation update;
C_e: The cost of bilinear maps;
$\mathbb{G}$: The cost of operation in group;
L_*: Bit length of element in *.

and modify more complicated access policies where simple addition and revocation update from our proposed schemes is not sufficient.

In terms of performance, the proposed schemes enjoy the constant-size ciphertext for users while ciphertexts produced in CP-AB-PRE are generally much longer. In addition, updated ciphertext produced in proposed schemes could be further updated without any length increment while most re-encrypted ciphertext in CP-AB-PRE can either not be re-encrypted again or be re-encrypted with linear increment in lenghth.

6.6 Intractability of the Proposed Assumptions

In this section, we provide the analysis of the intractability of (n, s)-aMSE-DDH problem. The intractability analysis is based on the analysis in the generic group model in [DP08].

6.6.1 (n, s)-aMSE-DDH

In this section, we prove the intractability of distinguishing the two distributions involved in the (n, s)-aMSE-DDH$_A$ problem (cf. Corollary 6.2, Section 6.2.2) and the intractability of the (n, s)-aMSE-DDH$_B$ problem (cf. Corollary 6.3, Section 6.2.2).

Proof of Corollary 6.2. To wrap up Corollary 6.2, we need to show that (n, s)-aMSE-DDH$_A$ problem fits in the framework of Theorem 2.30. As mentioned above, we consider our problem in the weakest case $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$ and pose $g_0 = g, h_0 = g^\beta$.

Our problem can be reformulated as decisional (P, Q, F)-GDHE Problem where

$$P = \begin{pmatrix} 1, \gamma, \ldots, \gamma^{n-2}, \\ \kappa \cdot \gamma \cdot f(\gamma), \\ \alpha, \alpha \cdot \gamma, \ldots, \alpha \cdot \gamma^{n-s+1}, \\ \omega \cdot \gamma, \omega \cdot \gamma^2, \ldots, \omega\gamma^{n-1}, \\ \beta, \beta \cdot \gamma, \ldots, \beta \cdot \gamma^{s-2}, \\ \beta\kappa \cdot g(\gamma), \beta\kappa \cdot \gamma \cdot g(\gamma), \ldots, \beta\kappa \cdot \gamma^{n-s} \cdot g(\gamma), \\ \beta\alpha, \beta\alpha \cdot \gamma, \ldots, \beta \cdot \alpha \cdot \gamma^n \\ \beta\omega, \beta\omega \cdot \gamma, \ldots, \beta\omega \cdot \gamma^n, \end{pmatrix}$$

$$Q = (1)$$

$$F = \beta\kappa \cdot f(\gamma).$$

We need to prove the independence of F from $\langle P, Q \rangle$. By making all possible products of two polynomials from P which are multiples of $\beta\kappa$, we want to prove that the sum of any polynomials from the list R below does not lead to F:

$$R = \begin{cases} \beta\kappa \cdot \gamma \cdot A(\gamma) f(\gamma) \\ \beta\kappa \cdot B(\gamma) g(\gamma) \\ \beta\kappa \cdot \gamma \cdot B(\gamma) g(\gamma) \\ \vdots \\ \beta\kappa \cdot \gamma^{s-2} \cdot B(\gamma) g(\gamma) \end{cases}$$

where A, B are polynomials in γ.

After simplifying the list R, it can be seen that if F is not independent of $\langle P, Q \rangle$ we can then derive $\gamma \cdot f(\gamma)$ from following list: $R' = \begin{cases} \gamma \cdot A(\gamma) f(\gamma) \\ B'(\gamma) g(\gamma) \end{cases}$ where A, B' are polynomials in γ with $0 \leq \deg A \leq s-2, 0 \leq \deg B' \leq n+s-4$.

Thus, we have the following equation:

$$f(\gamma) = \gamma \cdot A(\gamma) f(\gamma) + B'(\gamma) g(\gamma)$$

which can then be re-written into $(1 - \gamma \cdot A(\gamma)) f(\gamma) = B'(\gamma) g(\gamma)$ where $1 - \gamma \cdot A(\gamma) \neq 0$, $\deg B'(\gamma) \leq n+s-4$. Since f and g are coprime, we must have $g(\gamma) | (1 - \gamma \cdot A(\gamma))$. However, $\deg (1 - \gamma \cdot A(\gamma)) < \deg g(\gamma)$ will result in $1 - \gamma \cdot A(\gamma) = 0$, which contradicts with the fact $1 - \gamma \cdot A(\gamma) \neq 0$. □

Proof of Corollary 6.3. To wrap up Corollary 6.3, we need to show that (n, s)-aMSE-DDH$_B$ problem fits in Theorem 2.30 as well. As mentioned above, we consider our problem in the weakest case $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$ and pose $g_0 = g, h_0 = g^\beta$. Our

problem can be reformulated as Decisional (P, Q, f)-GDHE Problem where

$$P = \begin{pmatrix} 1, \gamma, \ldots, \gamma^{n-2}, \\ \kappa \cdot \gamma \cdot f(\gamma), \\ \alpha, \alpha \cdot \gamma, \ldots, \alpha \cdot \gamma^{2n-s}, \\ \omega \cdot \gamma, \omega \cdot \gamma^2, \ldots, \omega\gamma^{n-1}, \\ \beta, \beta \cdot \gamma, \ldots, \beta \cdot \gamma^{s-2}, \\ \beta\kappa \cdot g(\gamma) \\ \beta\alpha, \beta\alpha \cdot \gamma, \ldots, \beta\alpha \cdot \gamma^{n} \\ \beta\omega, \beta\omega \cdot \gamma, \ldots, \beta\omega \cdot \gamma^{s-1}, \end{pmatrix}$$
$$Q = (1)$$
$$F = \beta\kappa \cdot f(\gamma).$$

We need to prove the independence of F from $\langle P, Q \rangle$. By making all possible products of two polynomials from P which are multiples of $\beta\kappa$, we want to prove that the sum of any polynomials from the list R below does not lead to F:

$$R = \begin{cases} \beta\kappa \cdot \gamma \cdot A(\gamma) f(\gamma) \\ \beta\kappa \cdot B(\gamma) g(\gamma) \end{cases}$$

where A, B are polynomials in γ.

After simplifying the list R, it can be seen that if F is not independent of $\langle P, Q \rangle$ we can then derive $f(\gamma)$ from following list: $R' = \begin{cases} \gamma \cdot A(\gamma) f(\gamma) \\ B(\gamma) g(\gamma) \end{cases}$ where A, B are polynomials in γ with $0 \leq \deg A \leq s-2, 0 \leq \deg B \leq n-2$.

Thus, we have the following equation:

$$f(\gamma) = \gamma \cdot A(\gamma) f(\gamma) + B(\gamma) g(\gamma)$$

which can then be re-written into $(1-\gamma \cdot A(\gamma)) f(\gamma) = B(\gamma) g(\gamma)$ where $1-\gamma \cdot A(\gamma) \neq 0$, $\deg B(\gamma) \leq n-2$. Since f and g are coprime, we must have $g(\gamma) | (1 - \gamma \cdot A(\gamma))$. However, $\deg g = s$ and $\deg (1 - \gamma \cdot A(\gamma)) < \deg g(\gamma)$ will result in $1 - \gamma \cdot A(\gamma) = 0$, which contradicts with the fact $1 - \gamma \cdot A(\gamma) \neq 0$. □

6.7 Summary

In this chapter, we considered the problem of access policy update in ABE schemes, which make the ABE schemes become practical. When an ABE scheme is not equipped with efficient access policy update, it cannot be used in practice as policy update is an essential feature in the dynamic environment. We outlined some

trivial solutions including using AB-PRE system, and also pointed out the difference between access policy update and ciphertext re-encryption, which showed the importance of a general efficient access policy update mechanism. We presented notions of ciphertext-policy attribute-based encryption supporting attribute addition and revocation, and subsequently presented two new CP-ABE schemes featured with functionalities of adding and revoking attributes, respectively. We also proposed a new selective CPA model for CP-ABE with these new features. Finally, we also proved the security of our schemes. The proposed schemes are proven secure against selective CPA under the assumptions that the augmented Multi-Sequence of Exponents Decisional Diffie-Hellman problems are hard. The intractability of the aMSE-DDH problems is proved in generic group model within the framework of General Diffie-Hellman Exponent problem in [BBG05].

Chapter 7

Applications and Extensions

Applications of attribute-based encryption are largely beyond the scope of this thesis, but we pick two typical real-world scenarios to apply our proposed schemes. The first scenario is to establish Stand-Alone Authentication (SAA) mechanism in Fog Computing. In Fog Computing, fragile connection between Fog and Cloud causes problems of the authentication and authorization. We propose a traceable CP-ABE based on our key-delegation abuse resistance construction to handle not only the authentication and authorization problem but also the potential abuse of illegal key delegation and key duplication. The second scenario is to tackle attribute preservation problem within access policy update mechanism. Our previous proposed access policy update mechanism restrict attribute revocation capability by limiting how many attributes can be revoked. In this chapter, we propose an attribute revocation mechanism from a different construction concept with which encryptors can assign preserved attributes preventing further revocation.

7.1 Traceable CP-ABE in Fog Computing

7.1.1 Motivation

Recently, a new concept of Fog Computing has been proposed, which can enable applications on a large amount of devices connected in the Internet of Things to run directly at the network edge [Bon11]. In Fog Computing, services that are controlled from a Cloud can be hosted at end devices such as set-top-boxes, road side nodes or access points. The infrastructure of this new distributed computing allows users to enjoy the benefits of mobility support, geo-distribution, location-awareness and low latency as applications are designated to run close to them. Such Fog Computing concept connects user end smart devices such as smart phones, tablets, smart vehicles, which usually are restricted with computation power, battery and storage, with the Cloud at core by providing automated response. A three layer hierarchical service delivery model formed by end devices, Fog Computing and Cloud Computing that enhances quality of services and user experience makes Fog a successful extension of Cloud.

Since Fog Computing introduces multiple Fog devices between users and the Cloud, some security and privacy issues will impact the development of Fog Computing if not well addressed [QMC14, RCC17, CMCA17, DCY17, LCH16, DMC15,

MC14a, MC14b, MC13, MC12, QC14b, QC14a, QC13b, QC13c, QC13a]. One important security issue is that how to manage the problems of user authentication and authorization in Fog Computing. Stojmenovic et al. [SW14] have pointed out that different from Clouding computing [CDZ16] that can be well maintained Fog devices will face with unstable connectivity to the remote Cloud for distributing authentication information and collecting audit logs. This property of weak and fragile connectivity in Fog Computing reduced the reliability of performing an authentication protocol on remote Cloud authentication server. As a potential solution they introduced a new mechanism with Stand-Alone Authentication [HXB+14] to realise user authentication to adapt the unstable connectivity situation. However, to adopt Stand-Alone Authentication (SAA) the authentication information between users and designated Fog devices need to be protected. A common approach to share data securely with a designated party is encryption, but PKI-based authentication is not efficient in Fog Computing. Because in Fog Computing, which usually involves a large and dynamic information system for example the smart grid, there are a large number of Fog devices that provides different types of services in different locations, while users' access abilities to these Fog devices also vary due to different roles or how much money they paid. As an example, Alice can have SAA only with 'Fog devices of Type A OR Type B in All Areas', but another user Bob can have SAA with 'Fog devices of all types but only in Area C'. To overcome this obstacle, a recently introduced cryptographic primitive Attribute-based Encryption is adopted[YLL+15, YZL+16], which allows flexible one-to-many encryption without prior knowledge of who will be receiving the data.

To solve the authentication problem with SAA in Fog Computing, CP-ABE fits the situation perfectly. With CP-ABE, each user will be associated with a set of attributes ω with a private key and the Fog device will be labelled with an access policy $\mathbb{A}$ describing which kind of users can have SAA with it. A ciphertext on authentication information will be encrypted with an access policy $\mathbb{A}$ can only be decrypted by a private key for a user associated with a set of attributes ω that satisfies the access policy.

However, CP-ABE that suffers from key-delegation abuse or key-duplication abuse cannot be adopted to Fog Computing. In an environment that is implemented with Fog Computing, authentication information stored in user mobile devices can be easily duplicated or shared if a basic CP-ABE is adopted. In addition, splitting or mixing components of basic CP-ABE keys may lead to the generation of new illegal keys which can only worsen the situation. Theses misbehaviours should be warded off in a CP-ABE system that is employed in Fog Computing, and there needs to be an embedded subsystem to track malicious users if illegal duplication or sharing happens. Otherwise, the application of CP-ABE in Fog Computing will

be restrained.

7.1.2 Definition of Traceable CP-ABE

A traceable ciphertext-policy attribute-based encryption system consists of five algorithms: Setup, Enc, KeyGen, Dec, and Trace.

Setup($1^\lambda, \mathcal{P}$). The setup algorithm takes in the security parameters λ and the attribute universe $\mathcal{P}$. It outputs the public parameters params and a master secret key msk.

Encrypt(params, M, $\mathbb{A}$). The encryption algorithm takes in the public parameters params, the message M, and an access structure $\mathbb{A}$ over the universe of attributes. It will output a ciphertext CT such that only users with whose private keys associated with attribute sets which satisfy the access structure $\mathbb{A}$ can decrypt M. We assume that the ciphertext implicitly contains $\mathbb{A}$.

KeyGen(msk, W). The key generation algorithm takes as input the master secret msk and a set of attributes W. It outputs a private key sk associated with W.

Decrypt(params, CT, sk). The decryption algorithm takes as input the public parameters params, a ciphertext CT, which contains an access structure $\mathbb{A}$, and a private key sk, which is a private key for a set of attributes W. If the attribute set W satisfies the access structure $\mathbb{A}$ then the algorithm will decrypt the ciphertext and return a message M.

Trace(params, sk'). The trace algorithm takes as input the public parameters params and a valid private key sk'. It outputs the identity ID of the owner of the private key or $\perp$ if private key not valid.

7.1.3 Construction

In this subsection, we propose an application of our CP-ABE scheme against the property of key-delegation abuse in Fog Computing. A traceable CP-ABE scheme, which is a CP-ABE scheme that is equipped with a traitor tracing mechanism, is constructed based on our CP-ABE with key-delegation abuse resistance scheme. The main purpose of traitor tracing in ABE system is to guarantee that any user who illegally shared his/her private key can be traced. Many works have explored traceability in ABE schemes [LRK09, LHC+11, LCW13b, LCW13b]. Most of them focused on tracing new keys generated in collusive way, but few can prevent one user generating new workable keys in private. Based on our "key-delegation abuse" resistant CP-ABE scheme, we can obtain a *Traceable CP-ABE* system that can

trace privately generated illegal new keys with an extended attribute universe. Each user is given an attribute set that consists of attributes from the original attribute universe, which present his/her access right, as well as attributes from the extended attribute set, which indicate his/her identity. To be specific, we first let the original attribute universe be $\mathcal{P} := \{A_1, \ldots, A_n\}$ and a user identity space be $\mathcal{I}$ of size of 2^l, and we have the extended universe $\mathcal{P}' := \{A_1, \ldots, A_{n+l}\}$ in which attributes $\{A_1, \ldots, A_n\}$ are used for describing access right and attributes $\{A_{n+1}, \ldots, A_{n+l}\}$ are used to indicate identities. Next, when a private key for an attribute set ω (which only consists of attributes $\{A_1, \ldots, A_n\}$) and a user identity ID is queried, the user's identity ID is mapped to a distinct binary string $L_{ID} \in \{0,1\}^l$ by a collision-resistant hash function. According to the identity binary string L_{ID}, if the k-th digit is 1 the corresponding $(n+k)$-th attribute is added into a dummy attribute set ω_{ID}. The private key is then generated based on attribute set $\omega' = \omega \cup \omega_{ID}$. Since the decryption algorithm of our CP-ABE scheme requires corresponding key components for all attributes in the extended universe and our CP-ABE scheme is key-delegation abuse resistant, a user who wants to share his/her private key needs to give away the whole key, which will also give away the unique dummy attribute set. Thus, if a private key is shared, then the user will be traceable.

Using this technique, we can now describe our traceable CP-ABE construction as follows.

$\mathsf{Setup}(\lambda, \mathcal{I}, \mathcal{P}, \mathcal{I})$: Given a security parameter λ, a user identity space $\mathcal{I}$ of size of 2^l and an attribute universe $\mathcal{P}$ of size of n, the setup algorithm first sets the new universe $\mathcal{P}' := \{A_1, \ldots, A_{n+l}\}$. Next, it chooses a bilinear group $\mathbb{G}$ of prime order p. It then chooses random numbers $t_1, \ldots, t_{2(n+l)}, \alpha \in \mathbb{Z}_p$, random group generators $g_0, h_0 \in G$, and computes $Y = e(g_0, h_0)^\alpha, h_1 = h_0^{t_1}, \ldots, h_n = h_0^{t_{(n+l)}}$, $h_{n+1} = h_0^{t_{n+l+1}}, \ldots, h_{2(n+l)} = h_0^{t_{2(n+l)}}$. The public parameters are $\mathsf{params} = (h_1, \ldots, h_{2(n+l)}, Y, e, G, G_T, \mathcal{P})$. The master secret key is $\mathsf{msk} = (g_0, t_1, \ldots, t_{2(n+l)}, \alpha)$.

$\mathsf{Enc}(\mathsf{params}, M, \mathbb{A})$: To encrypt a message $M \in G_T$ with an access structure $\mathbb{A} = \bigwedge_{A_i \in S} i$ where $S \subset \mathcal{P}$, the following steps are taken. A random value $r \in \mathbb{Z}_p$ is chosen uniformly. The ciphertext is then created as: $CT = (\mathbb{A}, E' = MY^r, \{E_i = h_i^r\}_{A_i \in S}, \{E_i = h_{n+i}^r, E_i' = h_i^r\}_{A_i \in \mathcal{P}' \setminus S})$.

$\mathsf{KeyGen}(\mathsf{params}, \mathsf{msk}, W, ID)$: To generate a private key for attribute set $W \subseteq \mathcal{P}$ and a user identity $ID \in \mathcal{I}$ the following steps are taken. First, compute the identity binary string $L_{ID} = H(ID)$ and store the tuple of $\langle ID, L_{ID} \rangle$ into an internal list in the Trace algorithm. Next, a dummy attribute set W_{ID} is generated by adding $(n+k)$-th attribute if k-th digit of L_{ID} equals to 1.

Then, $n+l-1$ random values $x_1, \ldots, x_{n+l-1}$ are randomly chosen in $\mathbb{Z}_p$ and compute $x_n = \alpha - x_1 - \cdots - x_{n-1} \in Z_p$. The private key for the attribute set $\hat{W} = W \cup W_{ID}$:

$$sk = \left(\hat{W}, \{D_i = g_0^{\frac{x_i}{t_i}}\}_{A_i \in \hat{W}}, \{D_i = g_0^{\frac{x_i}{t_{n+i}}}\}_{A_i \in \mathcal{P}' \setminus \hat{W}} \right).$$

Dec(params, CT, sk) : Suppose that a ciphertext, CT, is encrypted with an access structure $\mathbb{A} = \bigwedge_{A_i \in S} A_i$ and we have a private key for attribute set $\hat{W} = W \cup W_{ID}$, where $S \subseteq W$.

Then, the ciphertext can be decrypted by following steps:

$$\begin{aligned}
&\prod_{A_i \in S \cup \{\mathcal{P}' \setminus W\}} e(D_i, E_i) \prod_{A_i \in W \setminus S} e(D_i, E_i') \\
&= \prod_{A_i \in W} e(g_0^{\frac{x_i}{t_i}}, h_i^r) \prod_{A_i \in \mathcal{P}' \setminus W} e(g_0^{\frac{x_i}{t_{n+i}}}, h_{n+i}^r) \\
&= \prod_{A_i \in W} e(g_0^{\frac{x_i}{t_i}}, h_0^{t_i r}) \prod_{A_i \in \mathcal{P}' \setminus W} e(g_0^{\frac{x_i}{t_{n+i}}}, h_0^{t_{n+i} r}) \\
&= e(g_0, h_0)^{r \sum_{A_i \in \mathcal{P}'} x_i} = e(g_0, h_0)^{\alpha r}. \\
&\frac{E'}{\prod_{A_i \in S \cup \{\mathcal{P}' \setminus W\}} e(D_i, E_i) \prod_{A_i \in W \setminus S} e(D_i, E_i')} \\
&= \frac{MY^r}{e(g_0, h_0)^{\alpha r}} = M.
\end{aligned}$$

Trace(params, sk') Let $sk' = \left(W', \{D_i'\}_{A_i \in W'}, \{D_i'\}_{A_i \in \mathcal{P}' \setminus W'}\right)$ be a valid decryption key, which means that $\prod_{A_i \in W'} e(D_i', h_i) \prod_{A_i \in \mathcal{P}' \setminus W'} e(D_i', h_{n+i}) = Y$. Then, it reconstructs the user identity binary string $L_{ID'} \in \{0,1\}^l$ by setting k-th digit to 1 if $(n+k) \in W'$; otherwise 0. Next, it searches the internal list for a tuple $\langle ID, L_{ID} \rangle$ where $L_{ID} = L_{ID'}$ and reveals the corresponding ID as the identity of the traitor. If the input is not a valid key, it outputs $\perp$.

Observe that the trace algorithm assumes that sk' has the prescribed form. It is possible to improve the trace algorithm to work with a black-box decryption box. A trivial construction would be to test the balck-box device with ciphertexts encrypted with access structure $\mathbb{A} = \bigwedge A_{n+k}$ where k-th digit of L_{ID} equals to 1 for all users' ID. As a reverse to the real encryption where none of attributes in $\{A_{n+1}, \ldots, A_{n+l}\}$ are used in access policies, the black-box device can only decrypt the ciphertext related to the same user ID from whose private key the black-box device is generated, since any key components dropped when generating the black-box device for hiding identity will disable the decryption ability of the black-box device.

7.1.4 Security Analysis

Theorem 7.1. *If the DBDH assumption holds, our Traceable CP-ABE scheme defined in Section 7.1.2 is secure in the sense of Definition 2.22.*

Proof. To prove the theorem, let us assume that there is an adversary $\mathcal{A}$ that can break our traceable CP-ABE scheme in the security game of IND-sCPA security model with non-negligible probability. We show how to use this adversary to construct an algorithm $\mathcal{B}$ which breaks the DBDH assumption.

For the algorithm $\mathcal{B}$ breaking the DBDH assumption, we let the challenger set the groups G and G_T of prime p with an efficient bilinear map, e and generator g. The challenger then flips a fair binary coin μ independent of $\mathcal{B}$'s view. If $\mu = 0$ the challenger sets $(A, B, C, Z) = (g^a, g^b, g^c, e(g,g)^{abc})$; otherwise $(A, B, C, Z) = (g^a, g^b, g^c, e(g,g)^z)$. At a high level, our simulation works as follows. We build a simulator that simulates the joint distribution consisting of adversary's view in its attack in the security game, and the hidden bit β which is not a part of the adversary's view.

We will show that if the input comes as $\mu = 0$, the simulation will be perfect, and so the adversary will launch its full ability breaking our CP-ABE. We will also show that if the input comes as $\mu = 1$, then the adversary's view is independent of β, and therefore the adversary's advantage is negligible. This immediately implies $\mathcal{B}$ distinguishing the distribution of its input tuple: run the simulator and adversary together, and if the simulator outputs β and the adversary outputs β', $\mathcal{B}$ outputs $\mu = 0$ if $\beta = \beta'$, and 1 otherwise.

We now give the details of the simulator.

The input to the simulator is $(p, G, G_T, e, g, A = g^a, B = g^b, C = g^c, Z)$.

Init During the *Init* phase, the simulator receives the challenge access structure $\mathbb{A}^* = \bigwedge_{A_i \in S^*} A_i$, where $S^* \subseteq \mathcal{P}$, from the adversary $\mathcal{A}$.

Setup Simulator set $n' = n + l$ and chooses random numbers υ, ν, θ_1, ..., $\theta_{n'}$, γ_1, ..., $\gamma_{n'} \in \mathbb{Z}_p$. Next, the simulator computes

$$
\begin{aligned}
&g_0 = g^{\upsilon}, h_0 = g^{\nu}, h_i|_{A_i \in \mathcal{P}'} = g^{\nu\theta_i} = h_0^{\theta_i}, \\
&h_{n'+i}|_{A_i \in S^*} = B^{\nu\gamma_i} = h_0^{b\gamma_i}, h_{n'+i}|_{A_i \in \mathcal{P} \setminus S^*} = g^{\nu\gamma_i} = h_0^{\gamma_i}, \\
&Y = e(A,B)^{\upsilon\nu} = e(g_0, h_0)^{ab}.
\end{aligned}
$$

Since $h_i = h_0^{t_i}$ and $h_{n'+i} = h_0^{t_{n'+i}}$ for each attribute $A_i \in \mathcal{P}'$, the simulator sets $t_i := \theta_i \in \mathbb{Z}_p$ for each attribute $A_i \in \mathcal{P}'$, $t_{n'+i} := b\gamma_i \in \mathbb{Z}_p$ for each attribute $A_i \in S^*$ and $t_{n'+i} := \gamma_i \in \mathbb{Z}_N$ for each attribute $A_i \in \mathcal{P}' \setminus S^*$. Since $Y = e(u_0, v_0)^{\alpha}$, the simulator also sets $\alpha := ab \in \mathbb{Z}_p$.

The simulated public parameters are $\mathsf{params} = (h_1, \ldots, h_{2n'}, Y, e, G, G_T, \mathcal{P})$. The master secret key is $\mathsf{msk} = (g_0, t_1, \ldots, t_{2n'}, \alpha)$.

Phase 1 The adversary $\mathcal{A}$ makes private key queries. The simulator responds to a query on a set of attributes $W \subseteq \mathcal{P}$ with an identity $ID \in \mathcal{I}$, where $S^* \not\subseteq W$, as follows. Observe that there must exist an attribute $A_k \in S^*$ such that $k \notin W$. The simulator first chooses such an attribute A_k. Next, the simulator chooses $r'_1, \ldots, r'_{n'-1} \in \mathbb{Z}_N$ uniformly at random and computes $r'_{n'} = -\sum_i r'_i$. Then the simulator sets $r_i := br'_i$ for each attribute $A_i \neq A_k \in \mathcal{P}'$ and $r_k := ab + br'_k$ for the attribute k. Fourth, the simulator checks if the pair $\langle ID, L_{ID} \rangle$ already exists in the internal list; if not it computes $L_{ID} = H(ID)$ and store the new pair $\langle ID, L_{ID} \rangle$ into the list. After L_{ID} is obtained the simulator sets a dummy attribute set W_{ID} generated by adding $(n+k)$-th attribute if k-th digit of L_{ID} equals to 1 and merges it with W so that $W' = W \cup W_{ID}$.

Finally, the simulator computes

$$\forall A_i \in W', D_i = B^{\frac{\upsilon r'_i}{\theta_i}} = (g^{\upsilon})^{\frac{br'_i}{\theta_i}} = g_0^{\frac{r_i}{t_i}}$$
$$\forall A_i \notin W', A_i \in S^*, i \neq k, D_i = g^{\frac{\upsilon r'_i}{\gamma_i}} = (g^{\upsilon})^{\frac{br'_i}{b\gamma_i}} = g_0^{\frac{r_i}{t_{n'+i}}}$$
$$\forall A_i \notin W', A_i \in S^*, i = k, D_k = A^{\frac{\upsilon}{\gamma_k}} \cdot g^{\frac{\upsilon r_k}{\gamma_k}} = g^{\frac{(ab+br'_k)\upsilon}{b\gamma_k}} = g_0^{\frac{r_k}{t_{n'+k}}}$$
$$\forall i \notin W', A_i \notin S^*, D_i = B^{\frac{\upsilon r'_i}{\gamma_i}} = (g^{\upsilon})^{\frac{br'_i}{\gamma_i}} = g_0^{\frac{r_i}{t_{n'+i}}}$$

and passes $sk = (W', \{D_i\}_{A_i \in \mathcal{P}'})$ onto $\mathcal{A}$.

Here we check the correctness of the simulated private key.

$$\sum_{A_i \in \mathcal{P}'} r_i = \sum_{A_i \neq A_k, A_i \in \mathcal{P}'} r_i + r_k = b \sum_{A_i \neq A_k, A_i \in \mathcal{P}'} r'_i + ab + br'_k = ab.$$

Challenge The adversary $\mathcal{A}$ outputs messages M_0, M_1. The simulator randomly generates a bit $\beta \in \{0, 1\}$ and sends $\mathcal{A}$ the challenge ciphertext:

$$CT^* = \Big(\mathbb{A}^*, C_m = M_\beta \cdot Z^{\upsilon\nu}, \{C_i = C^{\nu\theta_i} = {h_i}^c\}_{A_i \in S^*}, \{C_i = C^{\nu\gamma_i} = h^c_{n'+i}, C'_i = C^{\nu\theta_i} = h^c_i\}_{A_i \in \mathcal{P}' \setminus S^*} \Big).$$

Phase 2 $\mathcal{A}$ makes key queries, and the simulator responds as in Phase 1.

Guess Finally, the adversary outputs guesses β'. If $\beta = \beta'$, $\mathcal{B}$ outputs 0 indicating that $Z = e(g, g)^{abc}$; otherwise, it outputs 1.

Perfect Simulation: When $\mu = 1$ and $Z = e(g,g)^{abc}$, we have

$$C_m = M_\beta e(g,g)^{abc\upsilon\nu} = M_\beta e(g_0, h_0)^{abc} = M \cdot Y^c.$$

Thus, CT^* is a valid ciphertext for $\mathbb{A}^*$, and the public key and challenge ciphertext issued by the simulator comes from a distribution identical to that in the actual construction; however, we still must show that the private keys issued by the simulator are appropriately distributed. To show that the keys issued by the simulator are appropriately distributed, it suffices to show that, from A's view, the value g^a, g^b is uniformly random and independent. But this follows from the fact that g^a, g^b is chosen uniformly at random in G from the input.

Probability Analysis: We assume the adversary $\mathcal{A}$ breaks our CP-ABE scheme with non-negligible probability ϵ. If $Z = e(g,g)^{abc}$, then the simulation is perfect, and $\mathcal{A}$ will guess the bit β correctly with probability $1/2 + \epsilon$. Else, $Z = e(g,g)^z$ is uniformly random in G_T, and thus C_m is uniformly random and independent element in G_T. In this case, with probability $1 - 1/p$ the value of β is independent from $\mathcal{A}$'s view. Thus, we have that

$$\Pr[\mathcal{B}(A, B, C, Z) = 1] \geq \frac{1}{2} + \epsilon(1 - 1/p),$$

and

$$\mathsf{Adv}_{\mathcal{B}}^{\mathsf{DBDH}}(\lambda) \geq \epsilon(1 - 1/p).$$

This concludes the proof of Theorem. □

Theorem 7.2. *Our Traceable CP-ABE scheme is secure against Key-delegation Abuse Attacks of Definition 5.1 in the generic group model.*

Proof. To prove the traceable CP-ABE scheme is secure against Key-Abuse Attack in generic group model, it needs to prove that after extended with l attributes for a user identity space $\mathcal{I}$ of size of 2^l the adversary cannot generate a new private key that satisfies the winning conditions of the security game of Key-Abuse Attacks without any contradiction. In the setting of traceable CP-ABE, l attributes $\{A_{n+1}, \ldots, A_{n+l}\}$ that are used to indicate identities are added into the attribute universe. Each private key is generated with an extended set of attributes $W' = W \cup W_{ID}$ where attributes in W_{ID} do not affect the decryption procedure since no ciphertexts require attributes from $\{A_{n+1}, \ldots, A_{n+l}\}$ in its access policy. Therefore, the extended scheme does not gives the adversary any further advantage in breaking the security game of Key-Abuse Attacks. We give the detailed proof as following.

In the generic group model, the adversary can only manipulate group elements by using the canonical group operations, independent of the encoding for group elements. Thus if the adversary is given group elements $g^{\delta_1}, \ldots, g^{\delta_t} \in G$ as its only inputs, then each element of G output by the adversary must be of the form $g^{\pi(\delta_1,\ldots,\delta_t)}$, where π is a fixed multilinear polynomial.

Suppose the adversary gives a new private key sk^* with a decryption algorithm $Dec^*(\cdot)$ for an attribute set W^* and an identity ID^*, with which ciphertexts encrypted with $\mathbb{A}^* = \bigwedge_{A_i \in W^*} A_i$ can be decrypted. First, for a ciphertext CT encrypted under $\mathbb{A}^* = \bigwedge_{A_i \in W^*} A_i$ the new private key can decrypt M from C_m if it can be used to compute $Y^\kappa = e(g_0, h_0)^{\alpha\kappa}$. Thus, it contains a group element in $\mathbb{G}$ for each attribute in $\mathcal{P}'$ to pair the corresponding C_i (or C_i') in the ciphertext in bilinear map. We denote these group elements by D_i^* for attribute i in $\mathcal{P}'$ and the necessary structure of the new private key can be presented as $\left(\hat{W}^* = W^* \cup W_{ID^*}, \{D_i^*\}_{A_i \in \mathcal{P}'}\right)$.

After narrowing down the necessary construction for sk^*, we note that D_i^* needs to be constructed based on key components $D_i^{(j)}$ from j-th queried private key $sk^{(j)}$ for attribute set $W_j \cup W_{ID_j}$ since there is no other given group elements related to the unknown master secret key α for the adversary. Nevertheless, we also note that because of the difference of the queried attribute sets, for the same attribute A_i the key components $D_i^{(j)}$ might be generated based on different sets of group elements, which makes them irreconcilable to be combined together. Thus, the new private key sk^* can only depend on one queried private key sk_j where $W^* \subset W_j$. But this will result in that $sk*$ can be used to decrypt ciphertexts encrypted with W_j that is an attribute set beyond the supposed W^*, which contradicts the second condition in the security game's definition.

We consider two random encodings ψ_0, ψ_T of the additive group $\mathbb{Z}_p$ respectively, that is injective maps $\psi_0, \psi_T : \mathbb{Z}_p \to \{0,1\}^L$, where $L > 3\log(p)$. We write $G = \psi_0(x) : x \in \mathbb{Z}_p$,$G_T = \psi_T(x) : x \in \mathbb{Z}_p$. We are given oracles to compute the induced group action on G, G_T and an oracle to compute a non-degenerate bilinear map $e : G \times G \to G_T$. We refer to G as a generic bilinear group.

We now proceed with the proof, following the standard approach for generic groups with ψ_0, ψ_T, G, G_T defined as above. Let $g = \psi_0(1)$(we will write g^x to denote $\psi_0(x)$, and $e(g,g)^x$ to denote $\psi_T(x)$).

For any generic-group adversary, the security game against *key-delegation abuse* is considered carried out by a simulator as follows. For each group element seen or created by the adversary, this simulator keeps track of its discrete logarithm by means of a multivariate rational functions in the following indeterminate formal variables:

$$\sum = \{\upsilon, \nu\} \cup \{t_i\}_{A_i \in \mathcal{P}'} \cup \{r_i^{(j)}\}_{A_i \in \mathcal{P}', j \in [q]}.$$

The simulation also associates each group element with some rational function. For each distinct rational function in its collection, it inputs the value of the rational function to corresponding encoding ψ_0 or ψ_T and gives the result to the adversary as the encoding of that particular group element. The functions are associated with the group elements in the simulation as follows:

First, we suppose $g_0 = g^{\upsilon}, h_0 = g^{\nu}$. Let $n' = n + l$.

- Public parameters params generated by Setup
  $\mathsf{params} = (h_1, \ldots, h_{2n'}, Y)$.
  1. $\{\nu t_i\}_{A_i \in \mathcal{P}'}$, representing $h_i = h_0^{t_i} = g^{\nu t_i}$.
  2. $\{\nu t_{n'+i}\}_{A_i \in \mathcal{P}'}$, representing $h_i = h_0^{t_{n'+i}} = g^{\nu t_i}$.
- Private key components given by KeyGen. Let sk_j be the j-th queried private key for the attribute set W_j and the j-th identity.

$$sk_j = \left(\hat{W}_j = W_j \cup W_{ID_j}, \{D_i^{(j)} = g_0^{\frac{r_i^{(j)}}{t_i}}\}_{A_i \in \hat{W}_j}, \{D_i^{(j)} = g_0^{\frac{r_i^{(j)}}{t_{n+i}}}\}_{A_i \in \mathcal{P}' \setminus \hat{W}_j} \right)$$

  1. $\{\frac{\upsilon}{t_i} r_i^{(j)}\}_{j \in [q], A_i \in \hat{W}_j}$, representing $D_i^{(j)} = g_0^{\frac{r_i^{(j)}}{t_i}}$.
  2. $\{\frac{\upsilon}{t_{n+i}} r_i^{(j)}\}_{j \in [q], A_i \in \mathcal{P} \setminus \hat{W}_j}$, representing $D_i^{(j)} = g_0^{\frac{r_i^{(j)}}{t_{n+i}}}$.

Nevertheless, in the actual game, the values of the formal variables are chosen uniformly at random in $\mathbb{Z}_p$. Two distinct functions may in that case evaluate to the same value. The simulation is faithful to the standard interaction in a generic group, except in the event that two of the distinct functions evaluate to the same value on a random assignment to the formal variables. For any two distinct functions of the form listed above, the probability of this happening is at most $O(q)/p$, since the degree of distinct multivariate polynomials is at most $O(q)$. Since this probability is negligible, we ignore this case.

Now the adversary outputs a purported new private key sk^* for a new set of policy attributes W^* for the identity ID^* with a suitable decryption algorithm $Dec^*(\cdot)$. We first observe that to decrypt a ciphertext CT encrypted with an access structure $\mathbb{A} = \bigwedge_{A_i \in S} A_i$, where S is equal to or a subset of W^*. The new private key sk^* should contain a group element for each attribute to pair the corresponding group element C_i (or C_i') in the ciphertext in bilinear map for $Y^{\kappa} = e(g_0, h_0)^{\alpha\kappa}$. We denote these group elements by D_i^* and the necessary structure of the new private key can be presented as $(W^*, \{D_i^*\}_{A_i \in \mathcal{P}})$. On the other hand, as long as the new private key satisfies the winning conditions the adversary can construct the new key sk^* the way

it wants to make it look different, which means the adversary can construct the new private key component D_i^* using a linear combination of the functions listed above.

Here, we note that if the adversary tries to construct D_i^* using any functions other than $D_i^{(j)}$, then using this part of D_i^* in bilinear map will result in meaningless group element in $\mathbb{G}_T$ for decryption, which also needs to be eliminated by computing it separately; since it needs to be eliminated afterwards, we do not include it in following discussion.

Without loss of generality, we assume the new private key sk^* contains the following least structure for each attribute A_i:

$$\begin{aligned} D_i^* &= \pi_i(D_i^{(1)}, \ldots, D_i^{(q)}) := (D_i^{(1)})^{\beta_{i,1}}(D_i^{(2)})^{\beta_{i,2}} \cdots (D_i^{(q)})^{\beta_{i,q}} \\ &= u_0^{\frac{1}{t_i}\sum_{A_i \in W_j} \beta_{i,j} r_i^{(j)} + \frac{1}{t_{n+i}} \sum_{A_i \notin W_j} \beta_{i,j} r_i^{(j)}} \end{aligned}$$

where $\pi_i(D_i^{(1)}, \ldots, D_i^{(q)}) := (D_i^{(1)})^{\beta_{i,1}}(D_i^{(2)})^{\beta_{i,2}} \cdots (D_i^{(q)})^{\beta_{i,q}}$ represents a function in G using components $D_i^{(j)}$ from queried private keys.

Then we can represent D_i^* as $\frac{v}{t_i}\sum_{A_i \in W_j} \beta_{i,j} r_i^{(j)} + \frac{v}{t_{n+i}} \sum_{A_i \notin W_j} \beta_{i,j} r_i^{(j)}$.

To win in the game, D_i^* needs to meet following conditions:

1. $\sum_{A_i \in \mathcal{P}} \sum_{j \in [q]} \beta_{i,j} r_i^{(j)} = \alpha$.

2. $\forall A_i \in W^*, \sum_{i \notin W_j} \beta_{i,j} r_i^{(j)} = 0$.

3. $\forall A_i \notin W^*, \sum_{j \notin W_j} \beta_{i,j} r_i^{(j)} \neq 0$ and $\sum_{A_i \in W_j} \beta_{i,j} r_i^{(j)} = 0$.

The rest of our proof proceeds by assuming the new private key sk^* satisfies the conditions above, and obtaining a contradiction: that the new private key sk^* can be used to decrypt ciphertexts encrypted with a queried attribute set W_j which contradicts the second condition in the security game's definition.

Considering condition 1, $\sum_{A_i \in \mathcal{P}} \sum_{j \in [q]} \beta_{i,j} r_i^{(j)} = \alpha$. Since $\sum_i r_i^{(j)} = \alpha$ for $j \in [q]$ and $r_i^{(j)}$ is chosen uniformly at random in $\mathbb{Z}_p$, we have

$$\beta_{1,j} = \beta_{2,j} = \cdots = \beta_{n,j}.$$

We denote them by β_j.

Considering condition 2, for all $A_i \in W^*$, $\sum_{A_i \notin W_j} \beta_{i,j} r_i^{(j)} = \sum_{A_j, A_i \notin W_j} \beta_j r_i^{(j)} = 0$. Since $r_i^{(j)}$ is chosen uniformly at random in $\mathbb{Z}_p$, it can be concluded that

$$\text{if } \exists A_i \in W^* \text{ and } A_i \notin W_j, \beta_j = 0$$

which is equivalent to

$$\text{if } \beta_j \neq 0, W^* \subseteq W_j.$$

Considering condition 3, for all $A_i \notin W^*, \sum_{A_j \notin W_j} \beta_{i,j} r_i^{(j)} = \sum_{A_j \notin W_j} \beta_j r_i^{(j)} \neq 0$ and $\sum_{A_i \in W_j} \beta_{i,j} r_i^{(j)} = \sum_{A_i \in W_j} \beta_j r_i^{(j)} = 0$. Since $r_i^{(j)}$ is chosen uniformly at random in $\mathbb{Z}_p$, it can be concluded that

$$\text{if } \exists A_i \notin W^* \text{ and } A_i \in W_j, \beta_j = 0$$

which is equivalent to

$$\text{if } \beta_j \neq 0, W_j \subseteq W^*.$$

So W^* equals to a queried attribute set W_j, which results in either the adversary cannot generate a new key as $W^* \neq W_j$ for $j \in [q]$ or the new key will be able to decrypt ciphertexts encrypted with W_j as well since only one queried private key sk_j can be used. Therefore, our assumptions cannot be true. The adversary cannot successfully generate a new private key sk^* to win the game. □

7.1.5 Summary

This section presented an application of CP-ABE in the scenario of Fog Computing where a user interacts with many Fog devices that require different access privileges. In the scenario, Fog devices with different functionalities are distributed in a large area and users authenticate using smart devices with any viable private keys including those generated from illegal delegation or simple duplication. To tackle this problem, we proposed a traceable CP-ABE scheme based on the CP-ABE scheme with key-abuse delegation resistance. In proposed scheme, private keys cannot be split or combined to illegally delegate new keys. In addition, dummy attributes are used to represent user identities so that any successful authentication will leave a trace of user identity which then can be used for detection of private key duplications.

7.2 Access Policy Update with Preserved Attributes

7.2.1 Motivation

In CP-ABE, access control is enabled by access policies enforced with ciphertexts. Despite the fact that user private keys are associated with many descriptive attributes, certain attributes can be essential to an access policy so that the access control can work as designed. If a CP-ABE scheme that supports efficient access policy update but the essential attributes are not preserved, authorities may mistakenly revoke some from access policies which results in undesired access control

to the shared data. It can be seen that with a mature access policy update mechanism an encryptor should be able to preserve certain attributes in an access policy so that unintended recipients will not be able to decrypt the ciphertext after some attributes revoked.

Thus, in this section we provide the first construction of revocable CP-ABE with preserved attributes. The construction is provably secure under Decisional Bilinear Diffie-Hellman assumption in the introduced security model.

7.2.2 Construction

In this subsection, we present our revocable CP-ABE scheme that supports attributes preservation. In our construction revoked attributes will be replaced with certain dummy attributes in the access policy of a ciphertext, as well as the corresponding ciphertext components. These dummy attributes are owned by all users so that when an attribute is replaced by a dummy attribute the new ciphertext can then be decrypted. For simplicity, let this dummy attribute universe extends as $\mathcal{D} := \{A_{n+1}, \ldots, A_{2n}\}$, and $\mathcal{D}_i = \{A_{n+1}, \ldots, A_{n+i}\}$ for $i \leq n$. Hence, the general attribute universe for the construction will be $\mathcal{P}' = \mathcal{P} \cup \mathcal{D} = \{1, \ldots, 2n\}$.

7.2.2.1 Description

Our revocable CP-ABE scheme that supports attributes preservation follows the definition in Sec 6.2.1.

$\mathsf{Setup}(1^\lambda, \mathcal{P}')$: The setup algorithm chooses a bilinear group system $\mathbb{S} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(\cdot,\cdot))$ where $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$. It then randomly chooses a generator g as well as a set of exponents $t_{1,0}, \ldots, t_{2n,0}, t_{1,1}, \ldots, t_{2n-1,1}, \alpha, \beta \in \mathbb{Z}_p$.

The master secret key is then $\mathsf{msk} = (\alpha, t_{1,0}, \ldots, t_{2n,0}, t_{1,1}, \ldots, t_{2n-1,1})$ and the public parameters are

$$\mathsf{params} = (\mathbb{S}, g, Y = e(g,g)^\alpha, \{T_{i,j} = g^{t_{i,j}}\}_{i=1,\ldots,2n-1,j=0,1}).$$

$\mathsf{KeyGen}(\mathsf{msk}, W)$: To generate a private key for attribute set $W \subseteq \mathcal{P}$ the following steps are taken. Choose two polynomials $q_0(x)$ and $q_1(x)$ with degree $d_0 = d_1 = n-1$; set $q_0(x) = \alpha$ and $q_1(x) = q_0(2n)$. Randomly pick other $|W| + n - 1$ points to complete $q_0(x)$ as well as $|W| + n - 1$ points for $q_1(x)$. Compute the private key for W:

$$sk = (\{D_{i,0} = g^{\frac{q_0(i)}{t_{i,0}}}\}_{A_i \in W \cup \mathcal{D}_{n-1}}, \{D_{i,1} = g^{\frac{q_1(i)}{t_{i,1}}}\}_{A_i \in W \cup \mathcal{D}}).$$

$\mathsf{Enc}(\mathsf{params}, M, \mathbb{A}, l)$: Encryption with the AND-gate access policy $\mathbb{A} = \bigwedge_{A_i \in S} A_i$ with a set of attributes, message $M \in \mathbb{G}_T$ and the maximum allowed revocation number $l \leq k$ proceeds as follows. Let $S_1 \subseteq S$ be the set of fixed attributes and $S_2 \subseteq S$ be the set of revocable attributes. Randomly pick $r \in \mathbb{Z}_p$. The output ciphertext to users is then

$$CT = \begin{cases} S, \\ C_M = MY^r, \\ \{C_{i,0} = T_{i,0}^r\}_{A_i \in S_1 \cup \mathcal{D}_{n-|S_1|-1}}, \\ \{C_{i,1} = T_{i,1}^r\}_{A_i \in S_2 \cup \mathcal{D}_{n-|S_2|}}. \end{cases}$$

Afterwards, the algorithm computes $\forall i \in \{2n - |S_2| + 1, \ldots, 2n - |S_2| + l\}$: $C_{i,1} = T_{i,1}^r$ and send them to the proxy together with the ciphertext CT as CT_{p}.

$\mathsf{Update}(\mathsf{params}, CT_{\mathsf{p}}, \text{“}\mathsf{revoke}\text{”}, \mathcal{U})$: To revoke a set of attributes $\mathcal{U}$ from the AND-gate attribute set $S = S_1 \cup S_2$ of a ciphertext CT_{p}, where $\mathcal{U} \subset S_2$, the proxy proceeds the revocation algorithm as follows. For j-th attribute $A_i \in \mathcal{U}$, the corresponding ciphertext components $C_{i,1}$ is replaced with $C_{2n-|S_2|+j,1}$. Therefore, after revoking a set $\mathcal{U}$ of attributes, the AND-gate attribute set of the ciphertext will become $S' = S_1 \cup S_2'$ where $S_2' = S_2 \setminus \mathcal{U}$. The output ciphertext after revocation is then

$$CT = \begin{cases} S', \\ C_M = MY^r, \\ \{C_{i,0} = T_{i,0}^r\}_{A_i \in S_1 \cup \mathcal{D}_{n-|S_1|-1}}, \\ \{C_{i,1} = T_{i,1}^r\}_{A_i \in S_2' \cup \mathcal{D}_{n-|S_2|+|\mathcal{U}|}}. \end{cases}$$

$\mathsf{Dec}(sk, CT)$: Suppose a ciphertext CT that can be parsed as (S', C_M, $\{C_{i,0}\}_{A_i \in S_1 \cup \mathcal{D}_{n-|S_1|-1}}$, $\{C_i\}_{A_i \in S_2' \cup \mathcal{D}_{n-|S_2|}}$) and a private key for attribute set W, where W satisfies the access policy.

Let $S_1' = S_1 \cup \mathcal{D}_{n-|S_1|-1} \cup \{2n\}$. Then, the ciphertext can be decrypted by

following steps:

$$\prod_{A_i \in S_2' \cup \mathcal{D}_{n-|S_2|}} e(D_{i,1}, C_{i,1})^{\Delta_{A_i, S_2' \cup \mathcal{D}_{n-|S_2|}}(0)}$$

$$= e(g,g)^{q_0(2n)r}$$

$$(e(g,g)^{q_0(2n)r})^{\Delta_{A_{2n}, S_1'}(0)} \cdot e(g,g)^{q_0(2n)r}$$

$$= e(g,g)^{\alpha \cdot r}$$

$$\frac{C_M}{e(g,g)^{\alpha r}} = M$$

7.2.3 Security Analysis

We shall prove the following theorem.

Theorem 7.3. *If the DBDH assumption holds, our CP-ABE scheme defined in previous subsection is secure in the sense of Definition 6.1.*

Proof. To prove the theorem, let us assume that there is an adversary $\mathcal{A}$ that can break our CP-ABE scheme with non-negligible probability. We show how to use this adversary to construct an algorithm $\mathcal{B}$ which breaks the DBDH assumption.

For the algorithm $\mathcal{B}$ breaking the DBDH assumption, we let the challenger set the groups $\mathbb{G}$ and G_T of prime p with an efficient bilinear map, e and generator g. The challenger then flips a fair binary coin μ independent of $\mathcal{B}$'s view. If $\mu = 0$ the challenger sets $(A, B, C, Z) = (g^a,\ g^b,\ g^c,\ e(g,g)^{abc})$; otherwise $(A, B, C, Z) = (g^a, g^b, g^c, e(g,g)^z)$. At a high level, our simulation works as follows. We build a simulator that simulates the joint distribution consisting of adversary's view in its attack in the security game, and the hidden bit β which is not a part of the adversary's view.

We will show that if the input comes as $\mu = 0$, the simulation will be perfect, and so the adversary will launch its full ability breaking our CP-ABE. We will also show that if the input comes as $\mu = 1$, then the adversary's view is independent of β, and therefore the adversary's advantage is negligible. This immediately implies $\mathcal{B}$ distinguishing the distribution of its input tuple: run the simulator and adversary together, and if the simulator outputs β and the adversary outputs β', $\mathcal{B}$ outputs $\mu = 0$ if $\beta = \beta'$, and 1 otherwise.

We now give the details of the simulator.

The input to the simulator is $(p, \mathbb{G}, \mathbb{G}_T, e, g, A = g^a, B = g^b, C = g^c, Z)$.

Init During the *Init* phase, the simulator receives the challenge access structure $\mathbb{A}^* = \bigwedge_{A_i \in S^*} i$ from the adversary $\mathcal{A}$, where $S^* = S_1^* \cup S_2^* \subseteq \mathcal{U}$ and attributes

in S_1^* cannot be revoked while ones in S_2^* can be revoked.

Setup First simulator chooses random numbers $\gamma_{1,0}, \ldots, \gamma_{n,0}, \gamma_{1,1}, \ldots, \gamma_{n,1} \in \mathbb{Z}_p$. Next, the simulator defines $t_{i,0} = \gamma_{i,0}$ for $A_i \in S_1 \cup \mathcal{D}_{n-1-|S_1|}$, $t_{i,0} = b \cdot \gamma_{i,0}$ otherwise; $t_{i,1} = \gamma_{i,1}$ for $A_i \in S_2 \cup \mathcal{D}_{n-|S_2|}$, $t_{i,1} = b \cdot \gamma_{i,1}$ otherwise. The simulator then computes

$$T_{i,0} = \begin{cases} g^{t_{i,0}} = g^{\gamma_{i,0}}, & A_i \in S_1 \cup \mathcal{D}_{n-1-|S_1|} \\ g^{t_{i,0}} = B^{\gamma_{A_i,0}}, & \text{otherwise} \end{cases},$$

$$T_{i,1} = \begin{cases} g^{t_{i,1}} = g^{\gamma_{i,1}}, & A_i \in S_2 \cup \mathcal{D}_{n-|S_2|} \\ g^{t_{i,1}} = B^{\gamma_{i,1}}, & \text{otherwise} \end{cases},$$

$$Y = e(A, B) = e(g, g)^{ab}.$$

Since $Y = e(g, g)^{\alpha}$, the simulator implicitly sets $\alpha := ab \in \mathbb{Z}_p$.

The public parameter passed onto the adversary $\mathcal{A}$ is

$$\mathsf{params} = (\mathcal{U}, G, G_T, e, \{T_{i,j}\}_{1 \le i \le n, 0 \le j \le 1}).$$

Phase 1 The adversary $\mathcal{A}$ makes private key queries. The simulator responds to a query on W, where $W \not\models \mathbb{A}^*$, as follows. The simulator first defines two sets

$$\omega_0 = \begin{cases} S_1 \cap W \cup \mathcal{D}_{n-|S_1|-1}, & S_2 \not\subseteq W \\ S_1 \cap W \cup \mathcal{D}_{n-|S_1|-1} \cup \{2n\}, & S_2 \subseteq W \end{cases},$$

$$\omega_1 = S_2 \cap W \cup \mathcal{D}_{n-|S_2|}.$$

Observe that $|\omega_0| \le n - 1$. Next, the simulator defines a polynomial q_0 of degree $n-1$ such that $q_0(0) = a$. For $A_i \in \omega_0$ the procedure chooses a random point $\lambda_i \in \mathbb{Z}_p$ and sets $q_0(i) = \lambda_{i,0}$. After $|\omega_0|$ points set, it fixes the remaining $n - 1 - |\omega_0|$ points of q_0 randomly to completely define q_0. Now the simulator defines $Q_0(\cdot) = b \cdot q_0(\cdot)$, and computes

$$D_{i,0} = \begin{cases} g^{\frac{Q_0(i)}{t_{i,0}}} = g^{\frac{b\lambda_{i,0}}{\gamma_{i,0}}} = B^{\frac{\lambda_{i,0}}{\gamma_{i,0}}}, & A_i \in \mathcal{J}, \\ g^{\frac{Q_0(i)}{t_{i,0}}} = g^{\frac{bq_0(i)}{b\gamma_{i,0}}} = g^{\frac{q_0(i)}{\gamma_{i,0}}}, & otherwise, \end{cases}$$

where $\mathcal{J} = S_1 \cap W \cup \mathcal{D}_{n-|S_1|-1}$. (We note that $D_{i,0}$ can be computed in both situations since B and $g^a = A$ are both known by the simulator.)

In terms of $\{D_{i,1}\}$, the simulator defines a polynomial q_1 of degree $n-1$ such that $q_1(0) = q_0(2n)$ which can be either a known random number λ_{2n} if

$S_2 \subseteq W$ or defined by a group element in $\mathbb{G}$ associated with a computable with A. If $q_0(2n)$ is a known random number, the procedure then sets rest of the points randomly to completely fix q_1; otherwise chooses a random point $\lambda_{i,1}$ for $A_i \in \omega_1$ and then fixes the remaining $n-1-|\omega_1|$ points of q_1 to completely define q_1. After q_1 fixed, the simulator defines $Q_1(\cdot) = b \cdot q_1(\cdot)$ and computes

- If q_1 is completely known:

$$D_{i,1} = \begin{cases} g^{\frac{Q_1(i)}{t_{i,1}}} = g^{\frac{bq_1(i)}{\gamma_{i,1}}} = B^{\frac{q_1(i)}{\gamma_{i,0}}}, & A_i \in \omega_1, \\ g^{\frac{Q_1(i)}{t_{i,1}}} = g^{\frac{bq_1(i)}{b\gamma_{i,1}}} = g^{\frac{q_1(i)}{\gamma_{i,1}}}, & \text{otherwise}, \end{cases}$$

- Otherwise:

$$D_{i,1} = \begin{cases} g^{\frac{Q_1(i)}{t_{i,1}}} = g^{\frac{b\lambda_{i,1}}{\gamma_{i,1}}} = B^{\frac{\lambda_{i,1}}{\gamma_{i,0}}}, & A_i \in \omega_1, \\ g^{\frac{Q_1(i)}{t_{i,1}}} = g^{\frac{bq_1(i)}{b\gamma_{i,1}}} = g^{\frac{q_1(i)}{\gamma_{i,1}}}, & otherwise, \end{cases}$$

Finally, the simulator passes $sk = (W, \{D_{i,0}\}_{A_i \in W \cup \mathcal{D}_{n-1}}, \{D_{i,1}\}_{A_i \in W \cup \mathcal{D}})$ onto $\mathcal{A}$.

Challenge The adversary $\mathcal{A}$ outputs messages M_0, M_1 as well as the revocation attribute set $\mathcal{U}^*$. The simulator randomly generates a bit $\beta \in \{0,1\}$ and sends $\mathcal{A}$ the challenge ciphertext:

$$CT^* = \begin{cases} C_M^* = M_\beta \cdot Z, \\ \{C_{i,0}^* = T_{i,0}^c = C^{\gamma_{i,0}}\}_{A_i \in S_1 \cup \mathcal{D}_{n-|S_1|-1}}, \\ \{C_{i,1}^* = T_{i,1}^c = C^{\gamma_{i,1}}\}_{A_i \in S_2 \cup \mathcal{D}_{n-|S_2|}} \end{cases}$$

Phase 2 $\mathcal{A}$ makes key generation queries, and the simulator responds as in Phase 1.

Guess Finally, the adversary outputs guesses β'. If $\beta = \beta'$, $\mathcal{B}$ outputs 0 indicating that $Z = e(g,g)^{abc}$; otherwise, it outputs 1.

Probability Analysis:

Let $\mathcal{I} = (g, A, B, C, Z)$ be the input of the algorithm $\mathcal{B}$ and the adversary $\mathcal{A}$ break our CP-ABE scheme with advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sCPA}}(\lambda)$. Below we analyse the simulation in two cases.

Case 1 : $\mathcal{U}^* = \emptyset$

One can verify that in this case, if $\mu = 0$, $Z = e(g,g)^{abc}$, then $C_M^* = M_\beta \cdot e(g,g)^{abc} = M_\beta \cdot e(g,g)^{\alpha c}$. Therefore, the simulation of $\mathcal{B}$ is perfect, and the

adversary $\mathcal{A}$ will guess the bit β with its advantage. Hence, if $\mu = 0$ we have

$$|\Pr[\mathcal{B}(\mathcal{I}) = 0|\mu = 0] - \frac{1}{2}| = \mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sCPA}}(\lambda).$$

Else, if $\mu = 1$ and Z is uniformly random in G_T, C_M^* is uniformly random and independent in G_T, and the value of β is independent from $\mathcal{A}$'s view as well,

$$\Pr[\mathcal{B}(\mathcal{I}) = 0|\mu = 1] = \frac{1}{2}.$$

Thus, we have the advantage of $\mathcal{B}$ in solving the DBDH problem in Case 1 is

$$\begin{aligned}
&\mathsf{Adv}_{\mathcal{B}}^{\mathsf{DBDH}}(\lambda) \\
&\quad = |\Pr[\mathcal{B}(\mathcal{I}) = 0|\mu = 0] - \Pr[\mathcal{B}(\mathcal{I}) = 0|\mu = 1]| \\
&\quad \geq \mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sCPA}}(\lambda).
\end{aligned}$$

Case 2 : $\mathcal{U}^* \neq \emptyset$

In this case, we first show how a challenge ciphertext should be produced in a real game. Formally, the correct procedures are as follows.

Let $S' = \mathcal{U}^* \cup S$. The encryption algorithm $\mathsf{Enc}(\mathsf{params}, \mathbb{A}' = \bigwedge_{A_i \in S'} i, M_\beta, |\mathcal{U}^*|)$ is run to get CT^*. More precisely, it randomly picks $r \in \mathbb{Z}_p$ and computes,

$$CT^* = \begin{cases} C_M^*, \\ \{C_{i,0}^* = T_{i,0}^r\}_{A_i \in S_1 \cup \mathcal{D}_{n-|S_1|-1}}, \\ \{C_{i,1}^* = T_{i,1}^r\}_{A_i \in S_2 \cup \mathcal{U}^* \cup \mathcal{D}_{n-|S_2|-|\mathcal{U}^*|}} \end{cases}$$

as well as $\{C_{i,1} = T_{i,1}^r\}_{i \in \{2n-|S_2|-|\mathcal{U}^*|+1,\ldots,2n-|S_2|\}}$ for attribute revocation.

The revocation algorithm $\mathsf{Update}(\mathsf{params}, CT^*, \text{“}\mathsf{revoke}\text{”}, \mathcal{U}^*)$ is run to revoke the attribute set $\mathcal{U}^*$ from the access policy of the ciphertext CT^*. It updates attribute set S_2 by replacing the subset $\mathcal{U}^*$ by a set of dummy attributes of the same size $\{2n-|S_2|-|\mathcal{U}^*|+1, \ldots, 2n-|S_2|\}$, and substitute the corresponding $C_{i,1}$ of dummy attributes for the ones in the original ciphertext. Thus, the

output ciphertext is

$$CT^* = \begin{cases} C^*_M, \\ \{C^*_{i,0} = T^r_{i,0}\}_{A_i \in S_1 \cup \mathcal{D}_{n-|S_1|-1}}, \\ \{C^*_{i,1} = T^r_{i,1}\}_{A_i \in S_2 \cup \mathcal{D}_{n-|S_2|-|\mathcal{U}^*|}}, \\ \{C_{i,1} = T^r_{i,1}\}_{i \in \{2n-|S_2|-|\mathcal{U}^*|+1,\ldots,2n-|S_2|\}}. \end{cases}$$

$$= \begin{cases} C^*_M, \\ \{C^*_{i,0} = T^r_{i,0}\}_{A_i \in S_1 \cup \mathcal{D}_{n-|S_1|-1}}, \\ \{C^*_{i,1} = T^r_{i,1}\}_{A_i \in S_2 \cup \mathcal{D}_{n-|S_2|}}. \end{cases}$$

Now we assume that the randomness r used in producing CT^* is defined as $r = c$ and the challenge ciphertext CT' turns out to be as follows,

$$CT^* = \begin{cases} C^*_M = M_\beta \cdot Z, \\ \{C^*_{i,0} = T^c_{i,0} = C^{\gamma_{i,0}}\}_{A_i \in S_1 \cup \mathcal{D}_{n-|S_1|-1}}, \\ \{C^*_{i,1} = T^c_{i,1} = C^{\gamma_{i,1}}\}_{A_i \in S_2 \cup \mathcal{D}_{n-|S_2|}}. \end{cases}$$

It can be seen that if $\mu = 0$, $Z = e(g_0, h_0)^c$, the challenge ciphertext in a real game is exactly the same as the simulated challenge ciphertext. The simulated game would be a perfect simulation if it can be proved that the setting of r is indistinguishable from a real random value from the view of $\mathcal{A}$. It will suffice as c is random to $\mathcal{A}$. Thus, if $\mu = 0$ we have

$$|\Pr[\mathcal{B}(\mathcal{I}) = 0|\mu = 0] - \frac{1}{2}| = \mathsf{Adv}^{\mathsf{IND\text{-}sCPA}}_{\mathcal{A}}(\lambda).$$

On the other hand, if $\mu = 1$ and Z is a random element from G_T, C^*_M is random and independent from the view of $\mathcal{A}$,

$$\Pr[\mathcal{B}(\mathcal{I}) = 0|\mu = 1] = \frac{1}{2}.$$

Thus, we have the advantage of $\mathcal{B}$ in solving the DBDH problem in Case 2 is

$$\begin{aligned} \mathsf{Adv}^{\mathsf{DBDH}}_{\mathcal{B}}(\lambda) &= |\Pr[\mathcal{B}(\mathcal{I}) = 0|\mu = 0] - \Pr[\mathcal{B}(\mathcal{I}) = 0|\mu = 1]| \\ &\geq \mathsf{Adv}^{\mathsf{IND\text{-}sCPA}}_{\mathcal{A}}(\lambda). \end{aligned}$$

This completes the proof. □

7.2.4 Summary

This section gives a different approach for efficient access policy update mechanism considering practical usage and real-world design. The importance of the existence of attributes in an access policy, especially in an AND-gate access policy, varies since different attributes represent different types of access privileges. A new CP-ABE scheme is proposed where attributes in the access policy of a ciphertext can be designed as a preserved attribute. Such type of attributes cannot be revoked through the access policy update mechanism while other attributes are not affected. In the proposed solution, the ability of revoking attributes has been retrained with which encryptors can design access policies with more flexibility and rely on the update mechanism with further reassurance.

Chapter 8

Conclusion

This chapter summaries the main contributions and concludes the thesis. It also discusses several potential directions of future work.

8.1 Summary of Contributions

This thesis explores the attribute-based encryption aiming at exploiting innovative approaches and techniques for efficient and practical one-to-many encryption schemes. The contributions of the work are concluded as follows:

- Chapter 4 has focused on the dilemma of efficiency and expressiveness in attribute-based encryption. We propose a CP-ABE scheme with short ciphertexts that can support access policy of a threshold and an AND-gate. In the proposed scheme, encryptors can efficiently construct access policies with mandatory and optional attributes, and the encrypted message can only be recovered when all mandatory and certain number of optional attributes are included in the private key. This advanced feature is also favoured in many real world scenarios since it mitigates the problem in the assignment of key attributes. The proposed scheme takes a step forward beyond existing schemes and gives a modest but important advance in the field of attribute-based encryption.

- Chapter 5 has investigated the issue of key-delegation abuse in attribute-based encryption. The nature of attribute-based encryption results in the possibility of simple key-delegation, which can be friendly adopted for hierarchical key delegation or be maliciously used for illegal key generation. Concerning many scenarios where the latter usage causes severe undesired consequences, we defined a new security notion for the issue of key-delegation abuse and a formal security model against key-delegation abuse attacks. To tackle the problem, we proposed a CP-ABE scheme where a user cannot split or combine private key components to generate illegal keys for subsets of the original attribute set. The proposed scheme addresses the problem of key-delegation abuse by randomly breaking apart key randomness to pieces and combine them with key components preventing being used separately. Addressing the issue of key-delegation abuse helps enhance the security of applications that adopt attribute-based encryption for fine-grained access control.

- Chapter 6 has looked into practical need of access policy update mechanism in ABE systems. Most ABE schemes allow one-to-many encryption with static access control and only a few with the property of Proxy Re-encryption can update the access policy of a ciphertext with a re-encryption key. We proposed CP-ABE schemes where attributes can be efficiently added to (or revoked from) access policies of existing ciphertexts by a proxy server. The process of access policy update does not need any extra key from encryptors. Ciphertexts stored in server includes extra components that are used for access policy update, while a constant-sized part will be accessible for user-end decryption. We defined a new notion for this new mechanism and formalised the security requirements for the notion. The proposed solutions offer a novel approach to the problem of access policy update and make the ABE schemes become more versatile and practical.

- Chapter 7 has presented some applications and extensions of proposed schemes and mechanisms in Chapter 5 and 6 in real-world scenarios. The first part of this chapter focuses on the issue of key-delegation abuse in Fog Computing. We discussed how CP-ABE fits in the setting of Fog Computing and the key-delegation abuse could sabotage its security. We proposed a new traceable CP-ABE scheme with key-delegation abuse resistance. The proposed solution adopts the feature that user identities are embedded into indivisible private keys via dummy attributes. Differently from existing traceable CP-ABE schemes, the proposed scheme focused more on tracing new keys generated in private.

  The second part of this chapter deals with new challenges in applying the proposed proxy access policy update mechanism. Although the proposed scheme supports efficient access policy update, it leads to concerns on the subject of the extent of attribute revocation when updating an access policy. The mechanism embedded in the scheme proposed in Chapter 6 can only restrain the number of attributes that can be revoked, but it is more desired to restrain which ones can or cannot be revoked. Faced with this challenge, we proposed an efficient CP-ABE scheme with attribute revocation functionality in which encryptors can preserve certain attributes in the access policy. This solution is constructed with a different concept compared with schemes proposed in Chapter 6.

8.2 Future Work

The work proposed in this thesis can serve as the base for further research. Some of the potential directions are described in this section.

- In Chapter 4, the proposed CP-ABE scheme with short ciphertexts supports the access policy of an AND-gate and a threshold. On the one hand, it remains an

open problem to obtain an ABE scheme with constant-size ciphertexts supporting more expressive access policies. In spite of the difficulty between efficiency and expressiveness, it is worth trying to construct schemes for different access policies at the same level besides an AND-gate and a threshold that correspond to more practical situations. On the other hand, the security of proposed scheme is proven secure under the newly introduced assumption, which leads to further research on security proof under standard assumptions.

- In Chapter 5, the problem of key-delegation abuse is newly introduced and a CP-ABE scheme is constructed against key-delegation abuse attacks. A future work could be aimed at CP-ABE schemes with key-delegation resistance supporting more expressive access policies. In addition, the security proof against key-delegation abuse attacks is provided in the generic group model. It remains an open problem to prove security against key-delegation abuse attacks under standard assumptions.

- In Chapter 6, the problem of access policy update in ABE system is studied. The proposed schemes are embedded with efficient access policy update mechanism but support only AND-gate access policy. It remains an open problem to obtain a scheme integrated with efficient access policy update mechanism supporting more expressive access policies which can be proven secure under a more general computational assumption.

Bibliography

[AI09a] Nuttapong Attrapadung and Hideki Imai. Attribute-based encryption supporting direct/indirect revocation modes. In Matthew G. Parker, editor, *Cryptography and Coding, 12th IMA International Conference, Cryptography and Coding 2009, Cirencester, UK, December 15-17, 2009. Proceedings*, volume 5921 of *Lecture Notes in Computer Science*, pages 278–300. Springer, 2009.

[AI09b] Nuttapong Attrapadung and Hideki Imai. Conjunctive broadcast and attribute-based encryption. In Hovav Shacham and Brent Waters, editors, *Pairing-Based Cryptography - Pairing 2009, Third International Conference, Palo Alto, CA, USA, August 12-14, 2009, Proceedings*, volume 5671 of *Lecture Notes in Computer Science*, pages 248–265. Springer, 2009.

[AL10] Nuttapong Attrapadung and Benoît Libert. Functional encryption for inner product: Achieving constant-size ciphertexts with adaptive security or support for negation. In Nguyen and Pointcheval [NP10], pages 384–402.

[ALdP11] Nuttapong Attrapadung, Benoît Libert, and Elie de Panafieu. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In Catalano et al. [CFGN11], pages 90–108.

[ALO98] William Aiello, Sachin Lodha, and Rafail Ostrovsky. Fast digital identity revocation (extended abstract). In Hugo Krawczyk, editor, *Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings*, volume 1462 of *Lecture Notes in Computer Science*, pages 137–152. Springer, 1998.

[B96] Amos Beimel and . *Secure schemes for secret sharing and key distribution*. PhD Thesis, Technion-Israel Institute of technology, Faculty of computer science, 1996.

[BBG05] Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size ciphertext. In Cramer [Cra05], pages 440–456.

[BBS98] Matt Blaze, Gerrit Bleumer, and Martin Strauss. Divertible protocols and atomic proxy cryptography. In Kaisa Nyberg, editor, *Advances in Cryptology - EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May 31 - June 4, 1998, Proceeding*, volume 1403 of *Lecture Notes in Computer Science*, pages 127–144. Springer, 1998.

[BF01a] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In Kilian [Kil01], pages 213–229.

[BF01b] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In Kilian [Kil01], pages 213–229.

[BGK08] Alexandra Boldyreva, Vipul Goyal, and Virendra Kumar. Identity-based encryption with efficient revocation. In Ning et al. [NSJ08], pages 417–426.

[BLW09] Feng Bao, Hui Li, and Guilin Wang, editors. *Information Security Practice and Experience, 5th International Conference, ISPEC 2009, Xi'an, China, April 13-15, 2009, Proceedings*, volume 5451 of *Lecture Notes in Computer Science*. Springer, 2009.

[Bon11] Flavio Bonomi. Connected vehicles, the internet of things, and fog computing. In *The Eighth ACM International Workshop on Vehicular Inter-Networking (VANET), Las Vegas, USA*, pages 13–15, 2011.

[BSW07] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *2007 IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA*, pages 321–334. IEEE Computer Society, 2007.

[BSW11] Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. In Yuval Ishai, editor, *Theory of Cryptography - 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011. Proceedings*, volume 6597 of *Lecture Notes in Computer Science*, pages 253–273. Springer, 2011.

[CCL+13] Cheng Chen, Jie Chen, Hoon Wei Lim, Zhenfeng Zhang, Dengguo Feng, San Ling, and Huaxiong Wang. Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures. In Ed Dawson, editor, *Topics in Cryptology - CT-RSA 2013 - The Cryptographers' Track at the RSA Conference 2013, San Francisco,CA, USA,*

February 25-March 1, 2013. Proceedings, volume 7779 of *Lecture Notes in Computer Science*, pages 50–67. Springer, 2013.

[CDZ16] Kim-Kwang Raymond Choo, Josep Domingo-Ferrer, and Lei Zhang. Cloud cryptography: Theory, practice and future research directions. *Future Generation Comp. Syst.*, 62:51–53, 2016.

[CFGN11] Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors. *Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings*, volume 6571 of *Lecture Notes in Computer Science*. Springer, 2011.

[CMCA17] Niken Dwi Wahyu Cahyani, Ben Martini, Kim-Kwang Raymond Choo, and AKBP Muhammad Nuh Al-Azhar. Forensic data acquisition from cloud-of-things devices: windows smartphones as a case study. *Concurrency and Computation: Practice and Experience*, 29(14), 2017.

[CN07] Ling Cheung and Calvin C. Newport. Provably secure ciphertext policy ABE. In Ning et al. [NdVS07], pages 456–465.

[Cra05] Ronald Cramer, editor. *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*. Springer, 2005.

[CZF11] Cheng Chen, Zhenfeng Zhang, and Dengguo Feng. Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost. In Xavier Boyen and Xiaofeng Chen, editors, *Provable Security - 5th International Conference, ProvSec 2011, Xi'an, China, October 16-18, 2011. Proceedings*, volume 6980 of *Lecture Notes in Computer Science*, pages 84–101. Springer, 2011.

[DCY17] Christian D'Orazio, Kim-Kwang Raymond Choo, and Laurence T. Yang. Data exfiltration from internet of things devices: ios devices as case studies. *IEEE Internet of Things Journal*, 4(2):524–535, 2017.

[DMC15] Quang Do, Ben Martini, and Kim-Kwang Raymond Choo. A cloud-focused mobile forensics methodology. *IEEE Cloud Computing*, 2(4):60–65, 2015.

[DP08] Cécile Delerablée and David Pointcheval. Dynamic threshold public-key encryption. In David A. Wagner, editor, *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*, volume 5157 of *Lecture Notes in Computer Science*, pages 317–334. Springer, 2008.

[EMN+09] Keita Emura, Atsuko Miyaji, Akito Nomura, Kazumasa Omote, and Masakazu Soshi. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. In Bao et al. [BLW09], pages 13–23.

[GJPS08] Vipul Goyal, Abhishek Jain, Omkant Pandey, and Amit Sahai. Bounded ciphertext policy attribute based encryption. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Automata, Languages and Programming, 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, July 7-11, 2008, Proceedings, Part II - Track B: Logic, Semantics, and Theory of Programming & Track C: Security and Cryptography Foundations*, volume 5126 of *Lecture Notes in Computer Science*, pages 579–591. Springer, 2008.

[GLSW08] Vipul Goyal, Steve Lu, Amit Sahai, and Brent Waters. Black-box accountable authority identity-based encryption. In Ning et al. [NSJ08], pages 427–436.

[GPSW06] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, Ioctober 30 - November 3, 2006*, pages 89–98. ACM, 2006.

[GZC+12] Aijun Ge, Rui Zhang, Cheng Chen, Chuangui Ma, and Zhenfeng Zhang. Threshold ciphertext policy attribute-based encryption with constant size ciphertexts. In Willy Susilo, Yi Mu, and Jennifer Seberry, editors, *Information Security and Privacy - 17th Australasian Conference, ACISP 2012, Wollongong, NSW, Australia, July 9-11, 2012. Proceedings*, volume 7372 of *Lecture Notes in Computer Science*, pages 336–349. Springer, 2012.

[HJSS08] M. Jason Hinek, Shaoquan Jiang, Reihaneh Safavi-Naini, and Siamak Fayyaz Shahandashti. Attribute-based encryption with key cloning protection. *IACR Cryptology ePrint Archive*, 2008:478, 2008.

[HLR10] Javier Herranz, Fabien Laguillaumie, and Carla Ràfols. Constant size ciphertexts in threshold attribute-based encryption. In Nguyen and Pointcheval [NP10], pages 19–34.

[HN11] Junbeom Hur and Dong Kun Noh. Attribute-based access control with efficient revocation in data outsourcing systems. *IEEE Trans. Parallel Distrib. Syst.*, 22(7):1214–1221, 2011.

[HXB+14] Xinyi Huang, Yang Xiang, Elisa Bertino, Jianying Zhou, and Li Xu. Robust multi-factor authentication for fragile communications. *IEEE Transactions on Dependable and Secure Computing*, 11(6):568–581, 2014.

[IPN+09] Luan Ibraimi, Milan Petkovic, Svetla Nikova, Pieter H. Hartel, and Willem Jonker. Mediated ciphertext-policy attribute-based encryption and its application. In Heung Youl Youm and Moti Yung, editors, *Information Security Applications, 10th International Workshop, WISA 2009, Busan, Korea, August 25-27, 2009, Revised Selected Papers*, volume 5932 of *Lecture Notes in Computer Science*, pages 309–323. Springer, 2009.

[ITHJ09] Luan Ibraimi, Qiang Tang, Pieter H. Hartel, and Willem Jonker. Efficient and provable secure ciphertext-policy attribute-based encryption schemes. In Bao et al. [BLW09], pages 1–12.

[JSMG16a] Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo. Ciphertext-policy attribute based encryption supporting access policy update. In Liqun Chen and Jinguang Han, editors, *Provable Security - 10th International Conference, ProvSec 2016, Nanjing, China, November 10-11, 2016, Proceedings*, volume 10005 of *Lecture Notes in Computer Science*, pages 39–60, 2016.

[JSMG16b] Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo. Ciphertext-policy attribute-based encryption with key-delegation abuse resistance. In Joseph K. Liu and Ron Steinfeld, editors, *Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part I*, volume 9722 of *Lecture Notes in Computer Science*, pages 477–494. Springer, 2016.

[JSMG17a] Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo. Ciphertext-policy attribute-based encryption supporting access policy update and its extension with preserved attributes. *International Journal of Information Security*, Aug 2017.

[JSMG17b] Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo. Flexible ciphertext-policy attribute-based encryption supporting and-gate and threshold with short ciphertexts. *International Journal of Information Security*, May 2017.

[JSMG18] Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo. Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing. *Future Generation Comp. Syst.*, 78:720–729, 2018.

[Kil01] Joe Kilian, editor. *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*. Springer, 2001.

[LAL+15] Kaitai Liang, Man Ho Au, Joseph K. Liu, Willy Susilo, Duncan S. Wong, Guomin Yang, Yong Yu, and Anjia Yang. A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing. *Future Generation Comp. Syst.*, 52:95–108, 2015.

[LAS+14] Kaitai Liang, Man Ho Au, Willy Susilo, Duncan S. Wong, Guomin Yang, and Yong Yu. An adaptively cca-secure ciphertext-policy attribute-based proxy re-encryption for cloud data sharing. In Xinyi Huang and Jianying Zhou, editors, *Information Security Practice and Experience - 10th International Conference, ISPEC 2014, Fuzhou, China, May 5-8, 2014. Proceedings*, volume 8434 of *Lecture Notes in Computer Science*, pages 448–461. Springer, 2014.

[LCH16] Ming Di Leom, Kim-Kwang Raymond Choo, and Ray Hunt. Remote wiping and secure deletion on mobile devices: A review. *Journal of forensic sciences*, 61(6):1473–1492, 2016.

[LCLS09] Xiaohui Liang, Zhenfu Cao, Huang Lin, and Jun Shao. Attribute based proxy re-encryption with delegating capabilities. In Li et al. [LST+09], pages 276–286.

[LCLX09] Xiaohui Liang, Zhenfu Cao, Huang Lin, and Dongsheng Xing. Provably secure and efficient bounded ciphertext policy attribute based encryption. In Li et al. [LST+09], pages 343–352.

[LCW13a] Zhen Liu, Zhenfu Cao, and Duncan S. Wong. Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on ebay. In Ahmad-Reza Sadeghi, Virgil D. Gligor, and Moti Yung, editors, *2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013*, pages 475–486. ACM, 2013.

[LCW13b] Zhen Liu, Zhenfu Cao, and Duncan S. Wong. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures. *IEEE Trans. Information Forensics and Security*, 8(1):76–88, 2013.

[LFSW13] Kaitai Liang, Liming Fang, Willy Susilo, and Duncan S. Wong. A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security. In *2013 5th International Conference on Intelligent Networking and Collaborative Systems, Xi'an city, Shaanxi province, China, September 9-11, 2013*, pages 552–559. IEEE, 2013.

[LHC10] Song Luo, Jian-bin Hu, and Zhong Chen. Ciphertext policy attribute-based proxy re-encryption. In Miguel Soriano, Sihan Qing, and Javier López, editors, *Information and Communications Security - 12th International Conference, ICICS 2010, Barcelona, Spain, December 15-17, 2010. Proceedings*, volume 6476 of *Lecture Notes in Computer Science*, pages 401–415. Springer, 2010.

[LHC+11] Jin Li, Qiong Huang, Xiaofeng Chen, Sherman S. M. Chow, Duncan S. Wong, and Dongqing Xie. Multi-authority ciphertext-policy attribute-based encryption with accountability. In Bruce S. N. Cheung, Lucas Chi Kwong Hui, Ravi S. Sandhu, and Duncan S. Wong, editors, *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2011, Hong Kong, China, March 22-24, 2011*, pages 386–390. ACM, 2011.

[LLLS10] Xiaohui Liang, Rongxing Lu, Xiaodong Lin, and Xuemin Sherman Shen. Ciphertext policy attribute based encryption with efficient revocation. Technical report, Technical Report, University of Waterloo, 2010.

[LOS+10] Allison B. Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Henri Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010,*

29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings, volume 6110 of *Lecture Notes in Computer Science*, pages 62–91. Springer, 2010.

[LRK09] Jin Li, Kui Ren, and Kwangjo Kim. A2BE: accountable attribute-based encryption for abuse free access control. *IACR Cryptology ePrint Archive*, 2009:118, 2009.

[LRZW09] Jin Li, Kui Ren, Bo Zhu, and Zhiguo Wan. Privacy-aware attribute-based encryption with user accountability. In Pierangela Samarati, Moti Yung, Fabio Martinelli, and Claudio Agostino Ardagna, editors, *Information Security, 12th International Conference, ISC 2009, Pisa, Italy, September 7-9, 2009. Proceedings*, volume 5735 of *Lecture Notes in Computer Science*, pages 347–362. Springer, 2009.

[LST+09] Wanqing Li, Willy Susilo, Udaya Kiran Tupakula, Reihaneh Safavi-Naini, and Vijay Varadharajan, editors. *Proceedings of the 2009 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2009, Sydney, Australia, March 10-12, 2009*. ACM, 2009.

[LSW10] Allison B. Lewko, Amit Sahai, and Brent Waters. Revocation systems with very small private keys. In *31st IEEE Symposium on Security and Privacy, S&P 2010, 16-19 May 2010, Berleley/Oakland, California, USA*, pages 273–285. IEEE Computer Society, 2010.

[LV09] Benoît Libert and Damien Vergnaud. Adaptive-id secure revocable identity-based encryption. In Marc Fischlin, editor, *Topics in Cryptology - CT-RSA 2009, The Cryptographers' Track at the RSA Conference 2009, San Francisco, CA, USA, April 20-24, 2009. Proceedings*, volume 5473 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 2009.

[LXZZ13] Qinyi Li, Hu Xiong, Fengli Zhang, and Shengke Zeng. An expressive decentralizing KP-ABE scheme with constant-size ciphertext. *I. J. Network Security*, 15(3):161–170, 2013.

[MC12] Ben Martini and Kim-Kwang Raymond Choo. An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, 9(2):71–80, 2012.

[MC13] Ben Martini and Kim-Kwang Raymond Choo. Cloud storage forensics: owncloud as a case study. *Digital Investigation*, 10(4):287–299, 2013.

[MC14a] Ben Martini and Kim-Kwang Raymond Choo. Distributed filesystem forensics: Xtreemfs as a case study. *Digital Investigation*, 11(4):295–313, 2014.

[MC14b] Ben Martini and Kim-Kwang Raymond Choo. Remote programmatic vcloud forensics: A six-step collection process and a proof of concept. In *13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2014, Beijing, China, September 24-26, 2014*, pages 935–942. IEEE Computer Society, 2014.

[Mic96] Silvio Micali. Efficient certificate revocation. Technical report, Technical Report TM-542b, MIT Laboratory for Computer Science (March 22, 1996), 1996.

[Mil85] Victor S. Miller. Use of elliptic curves in cryptography. In Hugh C. Williams, editor, *Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer, 1985.

[Nao03] Moni Naor. On cryptographic assumptions and challenges. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 96–109. Springer, 2003.

[NdVS07] Peng Ning, Sabrina De Capitani di Vimercati, and Paul F. Syverson, editors. *Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007*. ACM, 2007.

[NNL01] Dalit Naor, Moni Naor, and Jeffery Lotspiech. Revocation and tracing schemes for stateless receivers. In Kilian [Kil01], pages 41–62.

[NP10] Phong Q. Nguyen and David Pointcheval, editors. *Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings*, volume 6056 of *Lecture Notes in Computer Science*. Springer, 2010.

[NSJ08] Peng Ning, Paul F. Syverson, and Somesh Jha, editors. *Proceedings of the 2008 ACM Conference on Computer and Communications Security, CCS 2008, Alexandria, Virginia, USA, October 27-31, 2008*. ACM, 2008.

[NYO09] Takashi Nishide, Kazuki Yoneyama, and Kazuo Ohta. Attribute-based encryption with partially hidden ciphertext policies. *IEICE Transactions*, 92-A(1):22–32, 2009.

[OSW07] Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-based encryption with non-monotonic access structures. In Ning et al. [NdVS07], pages 195–203.

[PTMW10] Matthew Pirretti, Patrick Traynor, Patrick D. McDaniel, and Brent Waters. Secure attribute-based systems. *Journal of Computer Security*, 18(5):799–837, 2010.

[QC13a] Darren Quick and Kim-Kwang Raymond Choo. Digital droplets: Microsoft skydrive forensic data remnants. *Future Generation Comp. Syst.*, 29(6):1378–1394, 2013.

[QC13b] Darren Quick and Kim-Kwang Raymond Choo. Dropbox analysis: Data remnants on user machines. *Digital Investigation*, 10(1):3–18, 2013.

[QC13c] Darren Quick and Kim-Kwang Raymond Choo. Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata? *Digital Investigation*, 10(3):266–277, 2013.

[QC14a] Darren Quick and Kim-Kwang Raymond Choo. Google drive: Forensic analysis of data remnants. *J. Network and Computer Applications*, 40:179–193, 2014.

[QC14b] Darren Quick and Kim-Kwang Raymond Choo. Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation*, 11(4):273–294, 2014.

[QM12] Wu Qiuxin and Zhang Miao. Adaptively secure attribute-based encryption supporting attribute revocation. *China Communications*, 9(9):22–40, 2012.

[QMC14] Darren Quick, Ben Martini, and Kim-Kwang Raymond Choo. *Cloud Storage Forensics*. Syngress Publishing / Elsevier, 2014.

[RCC17] Nurul Hidayah Ab Rahman, Niken Dwi Wahyu Cahyani, and Kim-Kwang Raymond Choo. Cloud incident handling and forensic-by-design: cloud storage as a case study. *Concurrency and Computation: Practice and Experience*, 29(14), 2017.

[RD13a] Y. Sreenivasa Rao and Ratna Dutta. Computationally efficient dual-policy attribute based encryption with short ciphertext. In Willy Susilo and Reza Reyhanitabar, editors, *Provable Security - 7th International Conference, ProvSec 2013, Melaka, Malaysia, October 23-25, 2013. Proceedings*, volume 8209 of *Lecture Notes in Computer Science*, pages 288–308. Springer, 2013.

[RD13b] Y. Sreenivasa Rao and Ratna Dutta. Recipient anonymous ciphertext-policy attribute based encryption. In Aditya Bagchi and Indrakshi Ray, editors, *Information Systems Security - 9th International Conference, ICISS 2013, Kolkata, India, December 16-20, 2013. Proceedings*, volume 8303 of *Lecture Notes in Computer Science*, pages 329–344. Springer, 2013.

[RS04] Phillip Rogaway and Thomas Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In Bimal K. Roy and Willi Meier, editors, *Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers*, volume 3017 of *Lecture Notes in Computer Science*, pages 371–388. Springer, 2004.

[SCG+16] Willy Susilo, Rongmao Chen, Fuchun Guo, Guomin Yang, Yi Mu, and Yang-Wai Chow. Recipient revocable identity-based broadcast encryption: How to revoke some recipients in IBBE without knowledge of the plaintext. In Xiaofeng Chen, XiaoFeng Wang, and Xinyi Huang, editors, *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, AsiaCCS 2016, Xi'an, China, May 30 - June 3, 2016*, pages 201–210. ACM, 2016.

[SGGR08] Jessica Staddon, Philippe Golle, Martin Gagné, and Paul Rasmussen. A content-driven access control system. In Kent E. Seamons, Neal McBurnett, and Tim Polk, editors, *IDtrust 2008, Proceedings of the 7th Symposium on Identity and Trust on the Internet, March 4-6, 2008, Gaithersburg, Maryland, USA*, volume 283 of *ACM International Conference Proceeding Series*, pages 26–35. ACM, 2008.

[Sho97] Victor Shoup. Lower bounds for discrete logarithms and related problems. In Walter Fumy, editor, *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*,

volume 1233 of *Lecture Notes in Computer Science*, pages 256–266. Springer, 1997.

[SK12] Hwajeong Seo and Howon Kim. Attribute-based proxy re-encryption with a constant number of pairing operations. *J. Inform. and Commun. Convergence Engineering*, 10(1):53–60, 2012.

[SW05] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In Cramer [Cra05], pages 457–473.

[SW14] Ivan Stojmenovic and Sheng Wen. The fog computing paradigm: Scenarios and security issues. In Maria Ganzha, Leszek A. Maciaszek, and Marcin Paprzycki, editors, *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems, Warsaw, Poland, September 7-10, 2014.*, pages 1–8, 2014.

[TDM12] Phuong Viet Xuan Tran, Thuc Nguyen Dinh, and A. Miyaji. Efficient ciphertext-policy abe with constant ciphertext length. In *2012 7th International Conference on Computing and Convergence Technology (ICCCT)*, pages 543–549, Dec 2012.

[Wat11] Brent Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In Catalano et al. [CFGN11], pages 53–70.

[WCLL12] Yongtao Wang, Kefei Chen, Yu Long, and Zhaohui Liu. Accountable authority key policy attribute-based encryption. *SCIENCE CHINA Information Sciences*, 55(7):1631–1638, 2012.

[XMLC13] Xingxing Xie, Hua Ma, Jin Li, and Xiaofeng Chen. New ciphertext-policy attribute-based access control with efficient revocation. In Khabib Mustofa, Erich J. Neuhold, A Min Tjoa, Edgar R. Weippl, and Ilsun You, editors, *Information and Communicatiaon Technology - International Conference, ICT-EurAsia 2013, Yogyakarta, Indonesia, March 25-29, 2013. Proceedings*, volume 7804 of *Lecture Notes in Computer Science*, pages 373–382. Springer, 2013.

[YLL+15] Yanjiang Yang, Joseph K. Liu, Kaitai Liang, Kim-Kwang Raymond Choo, and Jianying Zhou. Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data. In Günther Pernul, Peter Y. A. Ryan, and Edgar R. Weippl, editors, *Computer Security - ESORICS 2015 - 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part*

II, volume 9327 of *Lecture Notes in Computer Science*, pages 146–166. Springer, 2015.

[YRLL09] Shucheng Yu, Kui Ren, Wenjing Lou, and Jin Li. Defending against key abuse attacks in KP-ABE enabled broadcast systems. In Yan Chen, Tassos Dimitriou, and Jianying Zhou, editors, *Security and Privacy in Communication Networks - 5th International ICST Conference, SecureComm 2009, Athens, Greece, September 14-18, 2009, Revised Selected Papers*, volume 19 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 311–329. Springer, 2009.

[YWRL10] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Attribute based data sharing with attribute revocation. In Dengguo Feng, David A. Basin, and Peng Liu, editors, *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2010, Beijing, China, April 13-16, 2010*, pages 261–270. ACM, 2010.

[YZL+16] Yanjiang Yang, Haiyan Zhu, Haibing Lu, Jian Weng, Youcheng Zhang, and Kim-Kwang Raymond Choo. Cloud based data sharing with fine-grained proxy re-encryption. *Pervasive and Mobile Computing*, 28:122–134, 2016.

[ZZ11] Jiang Zhang and Zhenfeng Zhang. A ciphertext policy attribute-based encryption scheme without pairings. In Chuankun Wu, Moti Yung, and Dongdai Lin, editors, *Information Security and Cryptology - 7th International Conference, Inscrypt 2011, Beijing, China, November 30 - December 3, 2011. Revised Selected Papers*, volume 7537 of *Lecture Notes in Computer Science*, pages 324–340. Springer, 2011.